NOTE TO USERS

This reproduction is the best copy available.

UNIVERSITÉ DE MONTRÉAL

POUR UN MÉCANISME DE PROTECTION DIFFÉRENCIÉE UNIQUE CONTRE LA CONGESTION AINSI QUE LES PANNES: DIFFSERV*

CHRISTIAN AWAD
DÉPARTEMENT DE GÉNIE ÉLECTRIQUE
ÉCOLE POLYTECHNIQUE DE MONTRÉAL

THÈSE PRÉSENTÉE EN VUE DE L'OBTENTION
DU DIPLÔME DE PHILOSOPHIÆ DOCTOR
(GÉNIE ÉLECTRIQUE)
AVRIL 2009

Your file Votre référence
ISBN: 978-0-494-69192-2
Our file Notre référence
ISBN: 978-0-494-69192-2

UNIVERSITÉ DE MONTRÉAL

ÉCOLE POLYTECHNIQUE DE MONTRÉAL

Cette thèse intitulée:

POUR UN MÉCANISME DE PROTECTION DIFFÉRENCIÉE UNIQUE CONTRE LA CONGESTION AINSI QUE LES PANNES: DIFFSERV*

présentée par: AWAD Christian

en vue de l'obtention du diplôme de: Philosophiæ Doctor

a été dûment acceptée par le jury d'examen constitué de:

M. FRIGON Jean-François, Ph.D., président

Mme. SANSÒ Brunilde, Ph.D., membre et directrice de recherche

M. GIRARD André, Ph.D., membre et codirecteur de recherche

M. KASHYAP Raman, Ph.D., membre

M. HÉBUTERNE Gérard, Ph.D., membre

À mes parents.

REMERCIEMENTS

Je tiens à exprimer ma profonde reconnaissance envers mes directeurs de recherche, Prof. Brunilde Sansò et Prof. André Girard pour leur suivi et leur support continuels qui étaient indispensables à ma formation de chercheur. Je leur remercie pour m'avoir bénéficié de leur immense expertise en télécommunication, pour leurs conseils précieux et pour m'avoir fait confiance tout au long de cette thèse en me laissant orienter et mener à terme ce travail selon mes aspirations. Leur encouragement et leur encadrement constructif a énormément contribué à ma motivation et à mon désir de poursuivre ma quête de savoir et de contribuer à l'avancement de la science. Finalement, leur soutient moral et matériel m'était précieux et je ne saurais exprimer l'étendue de ma gratitude.

Je remercie grandement le Professeur Jean-François Frigon de m'avoir fait l'honneur de présider mon jury de thèse ainsi que les membres, Prof. Raman Kashyap et Prof. Gérard Hébuterne qui ont accepté de juger ce mémoire avec beaucoup d'attention et qui donneront à mon travail une valeur ajoutée à travers leurs recommandations et leurs remarques si importantes pour lesquels je serai très reconnaissant.

Une pensée particulière est adressée à tous mes professeurs pour m'avoir fourni le bagage académique nécessaire et prérequis à toutes mes activités de recherche. J'aimerai aussi remercier tous les techniciens pour leur support informatique et pratique quand j'en ai exprimé le besoin.

J'aimerai remercier aussi mes parents Elias et Ibtissam, mon frère Eddy, mes soeurs Nathalie et Mélanie, toute ma famille et mes amis, Maroun, Rony, Simon et bien d'autres pour leur soutient moral inconditionnel et leur encouragement incessant tout au long de mon cheminement académique.

À vous tous, je suis très reconnaissant, sans vous cette thèse n'aurai vu le jour et pour cela je souhaite vous être toujours une source de fierté et de satisfaction continuelle.

RÉSUMÉ

L'avènement de l'Internet multiservice met fin à l'ère du réseautage de nature meilleur effort. Cette nouvelle caractéristique est très souhaitable et prometteuse sur plusieurs plans mais elle reste sujette à la capacité du réseau de protéger chaque catégorie de trafic selon sa priorité et ses exigences en qualité de service. Quand le réseau est déployé sur une infrastructure optique, une des préoccupations des plus importantes est sa capacité de survie et le maintien d'un service adéquat à toutes les applications suite à une panne physique. Nous savons qu'une simple coupure de fibre provoque des pertes énormes en capacité de transmission et si laissée sans surveillance, elle peut causer des dégradations majeures dans la qualité de service perçue par les usagers du réseau. Bien qu'il existe déjà des mécanismes de protection physique qui sont conçus spécifiquement pour remédier à de telles situations, ces options sont généralement très coûteuses et difficilement adaptable aux besoins variés de chaque classe de trafic d'un réseau multiservice.

Nous proposons alors un modèle innovateur de protection différenciée du trafic, Diff-Serv*, qui permet de répondre aux exigences particulières en qualité de service et de protection de chacune des classes de trafic et qui introduit une robustesse accrue et des économies importantes en matière d'utilisation de ressources d'un réseau IP/WDM. Diff-Serv* se distingue par l'utilisation combinée de l'architecture des services différenciées à la couche logique d'un réseau et de la technique d'agrégation de liens ou canaux disjoints à sa couche physique.

Notre modèle de protection différenciée du trafic en cas de pannes à été soumis à l'épreuve, nous avons utilisé la simulation pour étudier sa performance et nous l'avons comparé à un modèle de protection *physique* homologue, DiffProtect. Les résultats montrent que Diff-Serv* permet *en moyenne* de garantir une meilleure protection que DiffProtect en cas de pannes simples et multiples. DiffProtect n'est plus performant que dans certaines situations de pannes et de trafic très particulières. Une évaluation subséquente de la fiabilité d'un réseau qui utilise DiffServ*, une étude de coût de son déploiement et une étude de

cas qui cible les réseaux MPLS-DiffServ TE confirment davantage la supériorité de Diff-Serv* par rapport à tout autre option de protection différenciée envisageable.

Nous rappelons que DiffServ* se base sur les techniques de différenciation de service de la couche *logique* pour protéger le trafic en cas de pannes de composantes optiques. Ceci est inédit puisque ces mêmes techniques sont originalement conçues que pour protéger le trafic en cas de congestion dans la couche logique. Alors pour démontrer définitivement que DiffServ* est réalisable et fonctionnel nous réalisons une expérience de déploiement pratique de DiffServ* en laboratoire à l'aide d'équipements de communication réel. Malgré les divergences techniques entre la modélisation théorique de DiffServ* et de son implémentation, DiffServ* est démontré performant, fiable, économique et réalisable en pratique.

Nous clôturons ce projet par une planification de déploiement ; cette dernière permet de généraliser le déploiement de DiffServ* à toute topologie IP/WDM et d'en dimensionner la couche logique. Notre procédure approche les situations qui requièrent la fiabilité spécifique de DiffProtect en offrant un modèle d'optimisation complet sur le déploiement de la protection MixProtect multicouche qui utilise DiffServ* et DiffProtect dans le même réseau.

ABSTRACT

Multiservice based networking is the next evolutionary step of the Internet in becoming a universal omni-communication tool. Although very desirable and promising, this new characteristic remains to a great extent subject to the capacity of the network to protect the Internet traffic in any circumstances according to its priority and its requirements in quality of service. When deployed on an optical infrastructure, one of the main concerns is the survivability of the network and its capacity to maintain an adequate level of service to all classes of traffic when physical failures take place. It is well known that with today's optical technologies such as WDM, a single fibre cut can result in a massive reduction in the network's overall transmission capacity and, if left unattended, the failure can lead to a catastrophic quality of service degradation from a user's standpoint. Although, many techniques have been developed to specifically remedy such situations, most are considered very expensive and not easily adaptable to the different needs of each traffic class in a multiservice network.

We therefore propose the novel differentiated protection model, DiffServ*, which allows us to meet the specific requirements in quality of service and protection of each traffic class and also introduces an increase in reliability and important savings in terms of resource use in IP/WDM networks. DiffServ* distinguishes itself by the combined mandatory use of the differentiated service architecture of a network's logical layer and a disjoint optical channel link bundling technique of its physical layer.

Our differentiated traffic protection model against failures has been extensively tested; we have used simulation to study its performance in comparison to that of its physical protection counterpart, DiffProtect. The results have clearly shown that DiffServ* quality of protection in both single and multiple failures is *on average* better than that of DiffProtect. Only in some very specific traffic and failure situations that DiffProtect is seen to take the upper hand. DiffServ*'s superiority over any other possible differentiated protection scheme has been subsequently proven by a detailed network reliability study, a thorough

cost evaluation of its deployment and a case study of its use within MPLS DiffServ-TE. We recall that DiffServ* relies mainly on a *logical* mechanism to differentiate and protection traffic in case of single or multiple simultaneous failures of optical components. This is innovative since this mechanism was originally intended for the protection of traffic against congestion in the logical layer. In order to definitively demonstrate that DiffServ* is in fact functional, we proceed with a practical deployment of DiffServ* using current network equipment. Despite all the technical disparities between the proposed theoretical model and its implementation, we show that DiffServ* is reliable, cost-effective and practically feasible.

We follow up these results and conclude this project with a deployment plan that dimensions the logical layer of any IP/WDM topology all the while generalizing the deployment of DiffServ* on all of its logical links. For all network situations that require the specific reliability guarantees of DiffProtect we append to the DiffServ* optimization model a multilayer protection solution that deploys both proposed models in the same network and optimizes the routing of traffic so that its protection is maximized.

TABLE DES MATIÈRES

DÉDICACE iv

REMERCIEMENTS v

RÉSUMÉ vi

ABSTRACT viii

TABLE DES MATIÈRES x

LISTE DES FIGURES xvi

LISTE DES NOTATIONS ET DES SYMBOLES xxi

LISTE DES TABLEAUX xxiv

LISTE DES ANNEXES xxv

INTRODUCTION 1

CHAPITRE 1 DÉFINITION DU PROJET 8

1.1 Le projet et les objectifs 8

1.2 Concepts de base 10

1.2.1 Pratique et utilité du groupement de liens dans un réseau IP/WDM 14

1.2.2 Problèmes liés au groupement de lien dans un réseau IP/WDM . . 17

1.3 Les modèles de protection 18

1.3.1 Le modèle DiffServ* 19

1.3.2 Protection de trafic dans DiffServ et DiffServ* 24

1.3.3 Le modèle DiffProtect 26

CHAPITRE 2 REVUE DE LITTÉRATURE 30
2.1 L'architecture DiffServ 31
2.1.1 Description de DiffServ et fonctionnement général 31
2.1.2 DiffServ dans un réseau IP/WDM 35
2.1.3 DiffServ dans la littérature 38
2.1.4 EF PHB et Trafic de Voix 42
2.1.5 AF PHB et Trafic Vidéo 44
2.2 Mécanismes de protection dans les réseaux IP/WDM 45
2.2.1 Mécanisme de protection dans les réseaux WDM 45
2.2.2 Mécanismes de protection et restauration du niveau IP 53
2.2.3 Routage IP/WDM de survie 57
2.3 Protection différenciée dans les réseaux 60
2.3.1 Probabilités de protection et protection différenciée 60
2.3.2 Disponibilité des ressources et protection différenciée 62
2.3.3 Protection différenciée par modélisation par arborescence 63
2.3.4 Qualité de service différenciée dans les réseaux WDM 64
2.3.5 Fiabilité différenciée 65
2.3.6 Qualité de protection 67
2.3.7 Qualité de fiabilité 68
2.3.8 Une qualité de rétablissement dynamique 70
2.3.9 Qualité de service différenciée dans les réseaux IP/WDM 71
2.4 Sommaire 72

CHAPITRE 3 MÉTHODOLOGIE, SIMULATIONS ET RÉSULTATS 74
3.1 Étude par simulation 74
3.2 Simulations d'un réseau à deux noeuds 76
3.2.1 Simulations avec trafic UDP 76
3.2.1.1 Sources de trafic 78

3.2.1.2 Détails de simulation et modélisation des pannes 82
3.2.1.3 Performance en cas de pannes 84
3.2.2 Simulation d'un réseau à deux noeuds et du trafic TCP 90
3.3 Simulations d'un réseau linéaire à quatre noeuds 94
3.3.1 Performance moyenne en mode normal 95
3.3.2 Performance moyenne en cas de pannes 102
3.3.3 Distributions de performance en cas de pannes 107
3.3.3.1 Distributions de performance de voix et de données . . 108
3.3.3.2 Distributions de performance de vidéo 109
3.3.3.3 Résumé 116
3.4 Simulations de grands réseaux maillés 117

CHAPITRE 4 ANALYSE DE FIABILITÉ, DE COÛTS ET ÉTUDE DE CAS . 128
4.1 Fiabilité des réseaux logiques protégés par DiffServ* 129
4.2 DiffServ*, DiffProtect et ressources optiques 132
4.2.1 Topologie étudiée 133
4.2.2 Demande de trafic IP et capacité de transmission optique 134
4.2.3 Nombre de longueurs d'ondes, DiffServ* et DiffProtect 135
4.2.4 Nombre de longueurs d'onde et topologie complète 138
4.2.4.1 Existence de 3 chemins disjoints entre deux routeurs . . 138
4.2.4.2 Existence de 2 chemins disjoints entre deux routeurs . . 139
4.2.4.3 Existence d'un seul chemin disjoint entre deux routeurs 139
4.2.4.4 Résultats 139
4.3 MPLS-DiffServ TE 141
4.3.1 Description de MPLS-TE 143
4.3.2 Rôle de DiffServ 144
4.3.3 Combiner MPLS-TE et DiffServ 144
4.3.4 Technique de groupement de liens dans un réseau MPLS-TE . . 145

4.3.5 MPLS DiffServ-TE, DiffServ* et DiffProtect 146
4.3.5.1 MPLS DiffServ-TE et DiffServ* 147
4.3.5.2 MPLS DiffServ-TE et DiffProtect 150
4.3.6 Assignation optique du trafic dans un réseau MPLS-DS-TE . . . 151
4.4 Fiabilité des réseaux MPLS-DS-TE 156
4.4.1 Simulation 160
4.4.1.1 Les flots du réseau 161
4.4.1.2 Les sources de trafic 161
4.4.1.3 Le scénario de pannes 162
4.4.1.4 Reroutage des LSP et capacité résiduelle du réseau . . 162
4.4.2 Résultats 163

CHAPITRE 5 DÉPLOIEMENT 170
5.1 DiffServ* et type de réseau visé 171
5.2 Description de l'expérience et des équipements réseaux nécessaires . . . 172
5.2.1 Générateurs et analyseurs de trafic 172
5.2.2 Configuration des commutateurs Atlas et Hercules. 175
5.2.2.1 Différenciation de service 177
5.2.2.2 Taux de service maximal du trafic de haute priorité . . 178
5.2.2.3 Ordonnancement prioritaire non offert 179
5.2.2.4 Partage de charge équilibré 180
5.3 Performance et résultats en cas de pannes 181
5.3.1 Résultats : EF-voix, AF-vidéo, BE-données 183
5.3.2 Résultats : EF-vidéo, AF-voix, BE-données 190
5.4 Déploiement Etherchannel de DiffProtect 196

CHAPITRE 6 DIFFSERV* ET DIFFPROTECT : PLANIFICATION ET DÉPLOIEMENT 198
6.1 Procédure de déploiement de la protection MixProtect 199

6.1.1 Données du problème 200
6.1.2 Dimensionnement DiffServ* de la topologie logique 201
6.1.3 Déploiement de DiffProtect et protection multi-niveau 203
6.1.3.1 Protection multi-niveau lien par lien 207
6.1.3.2 Routage du trafic en fonction de la protection 208
6.1.4 Différencier le routage pour maximiser la protection 208
6.2 Modélisation mathématique 210
6.2.1 Modèle 1 : Déploiement de DiffServ* 211
6.2.1.1 Variables et paramètres du modèle 211
6.2.1.2 Le modèle DiffServ* de routage et d'assignation de longueurs d'onde 215
6.2.2 Modèle 2 : Déploiement de DiffProtect 219
6.2.2.1 Les paramètres et variables de décision du modèle . . . 219
6.2.2.2 Le modèle de déploiement de DiffProtect 221
6.2.2.2.1 Les contraintes de la protection dédiée 222
6.2.2.2.2 Contraintes de la protection partagée 223
6.2.3 Modèle 3 : Routage de flot avec MixProtect 226
6.2.3.1 Notion de pénalité de protection 227
6.2.3.2 Les paramètres et variables du modèle 228
6.2.4 Le modèle d'optimisation 229
6.2.5 Technique de solution par détournement de flot 231
6.3 Implémentation et résultats 236
6.3.1 Réseau et données initiaux du modèle 237
6.3.2 Routage de flot, topologie logique et déploiement de DiffServ* . 237
6.3.3 Déploiement de DiffProtect 240
6.3.4 Reroutage des flots pour minimiser la pénalité 241

CONCLUSION 244

RÉFÉRENCES 247

ANNEXES 257

LISTE DES FIGURES

FIG. 1.1	Groupement de liens, partage de charge et routage de connexions IP/WDM	11
FIG. 1.2	Routage de connexion IP/WDM par chemin optique unique	12
FIG. 1.3	Routage de connections optiques sur chemins multiples	13
FIG. 1.4	Exemple d'un regroupement de liens IP/WDM	15
FIG. 1.5	Détails d'un noeud IP/WDM	16
FIG. 1.6	Modèle DiffServ*	20
FIG. 1.7	DiffServ* : modulation et commutation optique du trafic IP	21
FIG. 1.8	Avantages du déploiement du modèle DiffServ*	22
FIG. 1.9	Causes de congestion dans le modèle de protection DiffServ*	24
FIG. 1.10	Modèle DiffProtect	27
FIG. 1.11	DiffProtect : modulation et commutation optique du trafic IP	28
FIG. 2.1	Diagramme des fonctionnalités EDGE ou CORE de DiffServ	34
FIG. 2.2	Différenciation de trafic dans un réseau IP/WDM	36
FIG. 2.3	Protection par chemin	49
FIG. 2.4	Protection par lien	49
FIG. 2.5	Gestion des anomalies dans un réseau WDM.	50
FIG. 2.6	Protection dédiée par lien, exemple d'inefficacité.	51
FIG. 2.7	Routage de survie des connexions optiques	58
FIG. 2.8	Protection Partielle Différenciée	66
FIG. 3.1	Topologies IP, DiffServ* et DiffProtect, simulées à l'aide de NS-2.	77
FIG. 3.2	Débit d'une source de VoIP	79
FIG. 3.3	Distribution du trafic de voix sur un lien DiffProtect	80
FIG. 3.4	Distribution du trafic vidéo sur un lien DiffProtect	81
FIG. 3.5	Distribution du trafic de données sur un lien DiffProtect	81
FIG. 3.6	Distribution du débit sur un lien DiffServ*	82

FIG. 3.7 Taux de pertes moyen sous pannes 85
FIG. 3.8 Taux d'utilisation du lien DiffServ* en cas de pannes 86
FIG. 3.9 Délai moyen sous pannes 88
FIG. 3.10 Gigue moyenne sous pannes 90
FIG. 3.11 Taux de perte moyen, Trafic BE TCP 92
FIG. 3.12 Delai moyen, Trafic BE TCP 93
FIG. 3.13 Gigue Moyenne, Trafic BE TCP 93
FIG. 3.14 Réseau MixProtect (DS-DP-DS). 95
FIG. 3.15 Taux de pertes moyen, sans pannes 97
FIG. 3.16 Délai moyen, sans pannes 97
FIG. 3.17 Délai sur le lien (1,2) 99
FIG. 3.18 Délai sur le lien (2,3) 100
FIG. 3.19 Délai sur le lien (3,4) 101
FIG. 3.20 Gigue moyenne, sans pannes 102
FIG. 3.21 Taux de pertes moyen, avec pannes 103
FIG. 3.22 Délai moyen, avec pannes 106
FIG. 3.23 Gigue moyenne, avec pannes 107
FIG. 3.24 FDP du délai avec DP-DP-DP 109
FIG. 3.25 FDP du délai avec DP-DP-DS 110
FIG. 3.26 FDP du délai avec DP-DS-DS 111
FIG. 3.27 FDP du délai avec DS-DP-DS 111
FIG. 3.28 FDP du délai avec DP-DS-DP 112
FIG. 3.29 FDP du délai avec DS-DP-DP 113
FIG. 3.30 FDP du délai avec DS-DS-DP 114
FIG. 3.31 FDP du délai avec DS-DS-DS 115
FIG. 3.32 FDC du délai pour combinaisons commençant par DiffProtect . . 115
FIG. 3.33 FDC du délai pour combinaisons commençant par DiffServ* . . . 116
FIG. 3.34 Simulation d'un réseau en maille à noeuds. 119

FIG. 3.35 Taux de pertes moyen, flot B 122
FIG. 3.36 Délai moyenne, flot B 122
FIG. 3.37 Gigue moyenne, flot B 123
FIG. 3.38 Taux de perte moyen, réseau 124
FIG. 3.39 Délai moyen, réseau 125
FIG. 3.40 Gigue moyenne, réseau 126
FIG. 4.1 Routage et assignation de longueurs d'onde normal 130
FIG. 4.2 Routage et assignation de longueurs d'onde DiffServ* 130
FIG. 4.3 Réseau Optique 133
FIG. 4.4 Réseau Logique (IP) 134
FIG. 4.5 Calcul du nombre de canaux optiques 137
FIG. 4.6 Service, MPLS-DiffServ TE and Transport Planes 142
FIG. 4.7 MPLS DiffServ-TE : fonctionnement 148
FIG. 4.8 MPLS DiffServ-TE : fonctionnement avec DiffProtect 151
FIG. 4.9 LSR DiffServ*, DiffProtect 152
FIG. 4.10 DiffServ* : association LSP/canal optique 153
FIG. 4.11 DiffServ* : association LSP/canal optique suite après panne . . . 153
FIG. 4.12 DiffProtect : association LSP/canal optique 154
FIG. 4.13 DiffProtect : association LSP/canal optique après panne 155
FIG. 4.14 MPLS standard : association LSP/canal optique 155
FIG. 4.15 MPLS standard : association LSP/canal optique après pannes . . 156
FIG. 4.16 Propagation de panne localisée VS distribuée 158
FIG. 4.17 Retourage des LSP en cas de panne 159
FIG. 4.18 Taux de pertes moyen du réseau 165
FIG. 4.19 Délai moyen du réseau 167
FIG. 4.20 Gigue moyenne du réseau 169
FIG. 5.1 Réseau Etherchannel 173
FIG. 5.2 Débit normal de trafic EF, AF et BE 174

FIG. 5.3 Débit normal de trafic EF, AF et BE 175
FIG. 5.4 Partage de charge avant et après la qualité de service 176
FIG. 5.5 Sources et Destinations des flots EF, AF, BE 182
FIG. 5.6 Débit de trafic en cas de panne 184
FIG. 5.7 Débit de trafic en cas de panne 184
FIG. 5.8 Taux de pertes, EF et BE 186
FIG. 5.9 Délai, EF et BE 187
FIG. 5.10 Gigue, EF et BE 188
FIG. 5.11 Dégradation de performance vidéo visuelle, extrait de Starwars V 189
FIG. 5.12 Dégradation de performance vidéo visuelle, extrait de Matrix I . . 190
FIG. 5.13 Débit de trafic en temps normal (EF=vidéo) 191
FIG. 5.14 Débit de trafic en cas de panne (EF=vidéo) 191
FIG. 5.15 Débit de trafic en cas de panne(EF=vidéo) 192
FIG. 5.16 Taux de pertes, AF et BE 193
FIG. 5.17 Délai, AF et BE 194
FIG. 5.18 Gigue, AF et BE 195
FIG. 6.1 Initialisation : Demandes de trafic logique et topologie physique . 201
FIG. 6.2 Étape 1 : Déploiement de DiffServ*, dimensionnement et routage logique 202
FIG. 6.3 Étape2 : Probabilité de panne et déploiement de DiffProtect . . . 205
FIG. 6.4 Étape3 : Pénalité de protection, routage différencié et détournement de flots 210
FIG. 6.5 Un réseau IP/WDM à deux couches 212
FIG. 6.6 Solution de routage par lien VS. par chemin 232
FIG. 6.7 Topologie physique 237
FIG. 6.8 Topologie logique 238
FIG. 6.9 Routage DiffServ* des canaux optiques 240
FIG. 6.10 Routage DiffProtect des canaux optiques de protection 242

FIG. I.1 Deux mécanismes de partage de charge 258
FIG. I.2 Processus de réordonnancement avec le modèle DiffServ*. 260
FIG. I.3 Partage de charge et DiffServ 262
FIG. III.1 Routage par déflexion dans les réseaux OBS. 285
FIG. III.2 Routage par déflexion dans les réseaux DiffServ. 286
FIG. IV.1 Taux de pertes du flot 0 290
FIG. IV.2 Délai moyen du flot 0 291
FIG. IV.3 Gigue moyenne du flot 0 292
FIG. IV.4 Taux de pertes du flot 1 293
FIG. IV.5 Délai moyen du flot 1 294
FIG. IV.6 Gigue moyenne du flot 1 295
FIG. IV.7 Taux de pertes du flot 2 296
FIG. IV.8 Délai moyen du flot 2 297
FIG. IV.9 Gigue moyenne du flot 2 298

LISTE DES NOTATIONS ET DES SYMBOLES

AF :	Assured Forwarding
$ANOVA$:	ANalysis Of VAriance
BE :	Meilleur Effort (Best Effort)
BG :	BackGround Traffic
$CB\lambda$:	Class-Based Lightpath
CBQ :	Class-Based Queueing
CBS :	Commited Burst Size
$CORE$:	Routeur Intérieur d'un réseau DiffServ
$DiffServ$:	Services Différenciés (Differentiated Services)
$DiffServ*\ (DS)$:	Modèle de protection différenciée logique en cas de pannes
$DiffProtect\ (DP)$:	Modèle de protection différenciée physique en cas de pannes
DiR :	Differentiated Reliable connections
$DSCP$:	Identificateur de classe DiffServ (DiffServ Code Point)
$DWDM$:	Wavelength Division Multiplex
EBS :	Excess Burst Size
$EDGE$:	Routeur périphérique d'un réseau DiffServ
EF :	Expedite Forwarding
$FIFO$:	Premier Arrivé Premier Servi (First In First Out)
$IETF$:	Internet Engineering Task Force
$IntServ$:	Services Intégrés (Integrated Services)
IP :	Internet Protocol
$LACP$:	Link Agregation Control Protocol
LAN :	Local Area Network
LDP :	Label Distribution Protocol
LSP :	Label Switching Path

LSR :	Label Switching Router
MAN :	Metropolitan Area Network
$MaxTh$:	Maximum Threshold
MFP :	Maximum Failure Probability
$MinTh$:	Minimum Threshold
$MixProtect\ (MP)$:	Protection DiffServ*/DiffProtect Mixte
$MPLS$:	MultiProtocol Label Switching
$MRED$:	Multi Level-RED
OCh :	Optical Channel
OMS :	Optical Multiplex Section
$OSPF$:	Open Shortest Path First
OXC :	Commutateur Optique (Optical Cross-Connect)
PHB :	Comportement par saut (Per-Hop Behavior)
PRI :	Priority Queueing
QoP :	Qualité de Protection (Quality of Protection)
QoS :	Qualité de service (Quality of Service)
QoR :	Qualité de Fiabilité (Quality of Reliability)
$R-connections$:	Reliable connections
RED :	Random Early Detection
$RIO-C$:	RED In and Out - Coupled
$RIO-D$:	RED In and Out - Decoupled
RR :	Round Robin
$RSVP$:	Ressource reSerVation Protocol
RWA :	Routing and Wavelength Assignement
$srTCM$:	Single Rate Three Color Marking
TCL :	Tool Command Language

TCP :	Transport Control Protocol
TDM :	Time Division Multiplex
TE :	Traffic Engineering
$trTCM$:	Two Rate Three Color Marking
UDP :	User Datagram Protocol
WDM :	Wavelength Division Multiplex
WFQ :	Weight Fair Queueing
$WIRR$:	Weighted Interleaved Round Robin
$WRED$:	Weight RED
WRR :	Weighted Round Robin

LISTE DES TABLEAUX

TAB. 3.1 Nombre moyen de configurations de pannes qui affectent les liens logiques et le réseau 104

TAB. 3.2 Protection mixte des flots 121

TAB. 4.1 Fiabilité des liens logiques 132

TAB. 4.2 Utilisation des ressources : tableau récapitulatif 140

TAB. 4.3 Utilisation des ressources : tableau récapitulatif 141

TAB. 5.1 Sources et débit de trafic par machine 173

TAB. 5.2 Allocation Flot/Port, cas normal ou avec panne du port 22 183

TAB. 6.1 Matrice de trafic (Gbps) 238

TAB. 6.2 Routage des flot 239

TAB. 6.3 Matrice des taux d'utilisation des liens 239

TAB. 6.4 Matrice des positions de DiffProtect 241

TAB. 6.5 Détournement de flot, exemples 243

TAB. I.1 Performance de la décision aléatoire par groupe de paquets 263

LISTE DES ANNEXES

ANNEXE I PARTAGE DE CHARGE ET DÉSORDRE DES PAQUETS . . 257
I.1 Partage de charge dans le modèle DiffServ* 258
I.2 Solutions *DiffServ** au problème de partage de charge par paquet 261

ANNEXE II DISTRIBUTIONS DE DÉLAI ET GIGUE 264

ANNEXE III ROUTAGE PAR DEFLEXION POUR DIFFSERV 283
III.1 Routage par déflexion et réseaux OBS 283
III.2 Routage par déflexion pour DiffServ 285
III.3 DiffServ, DiffProtect et routage par déflexion 287

ANNEXE IV PERFORMANCE DES FLOTS 0, 1 ET 2 289

ANNEXE V CONFIGURATION DES COMMUTATEURS 299

INTRODUCTION

Développé par la communauté scientifique pour fournir des services de transfert de données et de courriers électroniques, le réseau Internet a grandement évolué depuis sa conception et sa mise en fonction. En plus des services de base, Internet exploite actuellement les grandes capacités de transmission d'une infrastructure optique pour fournir un large éventail de services plus avancés, de type multimédia et temps réel. Nous trouvons parmi ces derniers, la voix sur IP, la vidéoconférence, la vidéo sur demande et beaucoup d'autres. Ces nouveaux services sont beaucoup plus contraignants en termes de performance, ils requièrent des niveaux bien spécifiques en qualité de service (QdS) et ils imposent des limites strictes de taux de perte de données, de délai de bout en bout et de gigue, définie comme étant une mesure de la variation du délai. Pour assurer la bonne migration et la continuité de ces nouveaux services multimédias sur Internet, il est nécessaire que le réseau puisse garantir différents niveaux de qualité de service en tout temps et quelle que soit la nature des problèmes qui peuvent affecter son fonctionnement. Ces problèmes peuvent être regroupés en deux grandes catégories. La première caractérise l'état fonctionnel ou *en panne* des différents éléments du réseau. La deuxième tient compte du volume ou de la charge de trafic soumise aux ressources de transmission du réseau ; elle est reliée au niveau de *congestion* de ces différentes ressources.

Étant donné les débits très élevés des réseaux optiques, une simple coupure de fibre peut provoquer une perte colossale en capacité de transmission et une dégradation majeure de la qualité de service perçue par les usagers du réseau. Il est alors impératif de prévoir des mécanismes de protection contre ces failles éventuelles. Une technique directe, efficace et très coûteuse serait de dédoubler les ressources de transmission physique. Ainsi, la moitié de la capacité de transmission est utilisée pour servir le trafic en temps normal, l'autre moitié est réservée pour les temps de pannes. Parce que la protection contre une panne a lieu directement dans la couche physique, elle devient ainsi plus rapide et permet d'élimi-

ner les effets de cette panne sur le niveau logique supérieur. L'efficacité de cette technique entraîne par ailleurs un coût et une complexité de déploiement relativement élevés. Pour une même quantité de trafic, la taille du réseau doit être dédoublée et tous les flots de trafic sont dotés d'une protection dédiée même s'ils ne le requièrent pas. Ce problème peut être partiellement résolu en offrant à chaque type de trafic un niveau spécifique de protection optique. Cette méthode n'est toutefois pas sans difficulté puisqu'il existe toujours une partie de la capacité du réseau qui est exclusivement réservée à la protection et comme il est presque impossible de différencier le service entre les classes de trafic au niveau optique, il serait très difficile et complexe de différencier la protection à cette couche.

Il existe cependant plusieurs protocoles et architectures qui ont été explicitement développés pour assurer la différenciation de services à la couche logique du réseau Internet. Ces mécanismes de protection sont déjà disponibles et ont pour objectif de résoudre les problèmes de congestion et faciliter davantage l'intégration des nouveaux services dans le réseau Internet et permettre à celui-ci de devenir le premier réseau de communication multiservice (même omni service) et mondial.

Les deux principaux mécanismes de contrôle de congestion sont IntServ et particulièrement DiffServ. Tous deux aident à privilégier certains types de trafics par rapport à d'autres quand les ressources de transmission font défaut. IntServ se base sur la réservation de bout en bout des ressources pour chaque flot. Il offre deux classes de services, l'une avec ressources garanties, l'autre sans aucune garantie de service. Proposé par l'IETF, DiffServ en est un autre mécanisme qui figure parmi les architectures de différenciation de services les plus populaires. DiffServ est un mécanisme de protection différenciée, noeud par noeud, du trafic Internet contre les évènements de congestion qui peuvent avoir lieu en tout temps et qui résultent généralement d'une surutilisation temporaire de la capacité de transmission physique de certains éléments du réseau. Le fonctionnement de l'architecture DiffServ est simple. Elle permet de regrouper ensemble plusieurs flots de trafic qui requièrent des garanties similaires en QdS. Chaque regroupement forme une classe

de service et chaque classe possède une priorité. Les flots des applications temps réel de voix et de vidéo sont généralement regroupés sous les classes de hautes priorités, ceux des applications de transfert de données et de courriers électroniques sont généralement mis dans des classes de plus basses priorités. En cas de congestion, DiffServ assure que les flots des classes les plus prioritaires sont les premiers à être servis, ils ont ainsi un accès privilégié aux ressources de transmission, ils encourent le plus petit délai d'attente possible et profitent donc d'une meilleure qualité de service que ceux des classes les moins prioritaires. Nous obtenons ainsi une protection contre la congestion adéquate et adaptée à chaque catégorie de trafic qui utilise le réseau Internet. MPLS est un autre mécanisme qui a été introduit pour permettre une gestion améliorée des ressources de transmissions du réseau. Il permet un contrôle avancé sur le routage des flots de données au niveau logique. Couplé avec des algorithmes d'ingénierie de trafic (TE), MPLS permet aussi d'équilibrer la distribution de charge à travers le réseau. Ceci réduit le phénomène de surcharge de certaines régions du réseau par rapport à d'autres et permet une meilleure exploitation des ressources réseau disponibles. MPLS permet de dévier explicitement la trajectoire de certains flots prioritaires dans le but d'éviter certaines zones surchargées. La QdS offerte à certains types de trafic est de ce fait améliorée. Tous ces concepts prennent une importance majeure dans la conception d'un réseau de futures générations multiservice et efficace. Ces mécanismes réactifs et proactifs ont été conçus dans le but de contrer les surcharges temporelles de trafic, mais peuvent, dans certains cas, remédier aux pannes inévitables du réseau.

Dans ce qui précède, nous avons précisé la nécessité de prévoir des techniques de protection différenciée autant contre les pannes de la couche physique qu'en cas de congestion à la couche logique. Nous avons introduit brièvement les problèmes de complexité, de coûts, de gaspillage de ressources de transmission et des difficultés associées à la protection dédiée ou différenciée physique. Étant donné que la différenciation de services existe déjà à la couche logique des réseaux et est capable de protéger les flots de trafic les plus

prioritaires contre la congestion, nous voulons montrer qu'il est possible de réutiliser ses mêmes mécanismes pour protéger les différentes classes de trafic contre les pannes physiques aussi. L'objectif principal de ce projet se centre alors autour des points suivants :

- la conception d'une nouvelle technique de protection différenciée du trafic nommée DiffServ*. Cette dernière protège le trafic simultanément contre la congestion ainsi que contre les pannes du niveau physique. Cette technique doit être :
  - à faible complexité,
  - facile à déployer,
  - ne requiert aucun dédoublement des ressources de transmission physique (donc peu coûteuse),
  - assure un niveau de protection différencié et adéquat à chaque classe de trafic ;
- l'étude détaillée des avantages et inconvénients du modèle DiffServ* en comparaison avec un modèle homologue, DiffProtect de protection différenciée physique qui :
  - reproduit la protection DiffServ* au niveau physique,
  - peut combler au besoin les faiblesses du modèle DiffServ* ;
- étudier le déploiement conjoint des deux mécanismes de protection dans un réseau ;
- montrer la faisabilité et la performance du modèle DiffServ* avec de l'équipement réel ;
- proposer un modèle mathématique de déploiement combiné DiffServ*/DiffProtect dans un même réseau.

Le modèle DiffServ* de protection différenciée est basé sur l'architecture des services différenciés DiffServ de l'IETF. Ce modèle de protection reprend DiffServ comme partie intégrale et étend ces fonctionnalités pour devenir un mécanisme de protection non seulement contre la congestion, mais aussi contre les pannes physiques (principalement les pannes de liens). Bien que DiffServ n'ait pas été conçu pour cette tâche, nous montrons qu'il est possible, en s'aidant de la notion d'agrégation de canaux de transmission physique, de l'utiliser comme mécanisme de protection différenciée contre les pannes. Les avantages d'un tel modèle sont nombreux et d'une importance majeure puisqu'ils

apportent solution à plusieurs problèmes simultanéments.

D'un côté, nous proposons un mécanisme de protection *logique* et *unique* qui est capable de protéger rapidement et efficacement les flots de trafic de hautes priorités contre les effets de la congestion *et* des pannes. D'un autre côté, la protection DiffServ* est pratiquement immédiate et ne requiert aucune réservation de ressources de protection supplémentaires. Les débits élevés de la couche physique sont donc entièrement utilisés pour transmettre le trafic, ce qui a donc pour effet de maximiser le taux d'utilisation et d'éviter le gaspillage des ressources du réseau. D'autant plus, comme DiffServ et la notion d'agrégation de liens sont courants et se trouvent déjà dans les réseaux de télécommunications actuels, le déploiement de la protection DiffServ* se fait pratiquement *sans effort*, sans coûts supplémentaires et permet de garantir *un meilleur niveau de fiabilité différenciée* en cas de pannes que tout autre mécanisme de protection physique. Les avantages d'un déploiement généralisé du modèle DiffServ* sur tous les liens du réseau sont :

- la couche logique est pratiquement immunisée contre les pannes de liens et le recours aux mécanismes lents et complexes de reroutage après pannes est de ce fait minimisé ;
- l'augmentation soudaine de la demande de trafic et les pannes physiques causent toutes deux une congestion, ce qui limite l'effet des problèmes de réseau à un seul symptôme, la congestion, donc un seul traitement, DiffServ ;
- un seul mécanisme pour protéger le trafic quelle que soit sa priorité et les conditions du réseau, nous avons donc une complexité d'exploitation réduite et un bas coût de déploiement.

Comme nous le montrons au cours des premiers chapitres de cette thèse, le modèle DiffServ* a été mis à l'épreuve en utilisant la méthode de simulation. Le logiciel de simulation NS-2 a été utilisé. Deux modèles de simulation ont été élaborés, le premier pour simuler la protection différenciée réalisée avec le protocole DiffServ, le deuxième pour simuler la protection physique différenciée, DiffProtect. Le deuxième modèle combine plusieurs

mécanismes de protection physique pour offrir à chaque classe de trafic un niveau de fiabilité adéquat. Nous avons évalué la performance des deux modèles de simulations dans plusieurs réseaux de différentes tailles et dans différentes situations de pannes simples et multiples. Les résultats sont publiés dans (Sansò et al., 2006; Awad et al., 2008) et montrent clairement que la protection qui utilise DiffServ est capable de rivaliser sinon surpasser la protection physique dans la majorité des situations de pannes. Ceci est un résultat très important et même contre-intuitif, car il montre que si un réseau est conçu adéquatement, il est possible de faire confiance à DiffServ* pour protéger le trafic de haute priorité en cas de pannes simples et même multiples du niveau de la couche de transmission physique. Avec DiffServ*, l'ajout de ressources en guise de protection au niveau physique et la planification proactive contre les pannes ne sont pas nécessaires. Ceci permet non seulement de réduire le coût d'installation des réseaux de télécommunication, mais de simplifier et réduire la complexité de leur maintenance car un seul mécanisme logique et simple, DiffServ*, suffit pour protéger le trafic contre la congestion en temps normal et contre les effets des pannes en cas de problèmes.

La présente thèse est divisée comme suit. Le chapitre 1 porte sur la définition et la description détaillée des deux modèles de protection DiffServ* et DiffProtect. Une revue de la littérature détaillée est explicitée dans le deuxième chapitre. Le chapitre 3 porte sur les simulations et les résultats obtenus ; ils montrent l'efficacité du modèle DiffServ* quand comparé à la protection physique. Le chapitre 4 comprend une étude de fiabilité et de coût de déploiement ainsi qu'une étude de cas sur l'utilisation de DiffServ* et DiffProtect dans un réseau MPLS-DiffServ-TE sélectionné comme candidat pour le réseau Internet de future génération. Nous montrons dans ce chapitre que le déploiement de DiffServ* en tant que mécanisme de protection requiert une modification dans la façon dont les ressources de transmission physique sont utilisées. Le trafic entre deux noeuds doit être partagé et envoyé sur plusieurs chemins disjoints qui relient ces deux routeurs. Les chemins physiques disjoints sont agrégés ensemble pour former un lien logique unique sur lequel DiffServ*

fonctionne. Cette modification requiert une quantité supplémentaire de ressources mais elle demeure inférieure à celle requise par les mécanismes de protection traditionnels et de DiffProtect. Les résultats de cette étude sont aussi montrés dans (Awad et al., 2008). Une étude de déploiement pratique est présentée dans le chapitre 5. Une modélisation mathématique du projet est présentée dans le chapitre 6.

CHAPITRE 1

DÉFINITION DU PROJET

Ce chapitre décrit en détail les objectifs principaux du projet. Il fournit aussi une description détaillée des modèles de protection différenciée proposés ainsi que les concepts de base utilisés.

1.1 Le projet et les objectifs

La littérature montre la nécessité d'utiliser des mécanismes de protection rapides et surtout différenciés au niveau WDM. Cette nécessité est justifiée par le fait qu'aucune couche supérieure logique, notamment IP, n'est capable de garantir une restauration de service rapide digne de chaque classe de trafic. L'objectif principal de ce projet est de montrer que l'architecture DiffServ, un mécanisme logique de protection contre la congestion, peut être utilisée comme un mécanisme de protection contre les pannes des équipements optiques. Nous proposons d'abords un modèle de protection différenciée, le modèle DiffServ*. La nouveauté introduite par ce modèle est qu'il se base sur le concept de groupement liens (*Link Bundling*) et un routage spécial des connexions IP sur la topologie WDM (*Connexion Mapping*). Ces concepts sont expliqués en détail dans la section 1.2. Cette architecture des services différenciés permet une protection logique instantanée du trafic de hautes priorités contre les pannes simples et multiples de chemins optiques. La performance du modèle DiffServ* est par la suite comparée à celle d'un autre modèle de protection différenciée physique, DiffProtect. Ce dernier se base sur les mêmes concepts que DiffServ* mais requiert en plus un routage *différencié* des connexions logiques sur la topologie physique et garantit à chaque trafic une protection WDM qui lui est appropriée.

Le modèle DiffServ* offre alors une approche originale et avantageuse qui assure une protection essentiellement logique efficace et instantanée aux trafics de hautes priorités sans aucun recours à des mécanismes de protection physique. L'efficacité de DiffServ* montre que la protection optique peut ainsi être remplacée par un mécanisme de protection unique à moindre coût qui opère à la couche IP.

Comme nous le montrons dans le chapitre 3, nous utilisons premièrement l'approche par simulation pour étudier et comparer la performance des deux modèles DiffServ* et DiffProtect. Bien que la littérature propose de mesurer l'effet des pannes en termes de probabilité d'interruption de service ou temps de restauration, ce projet propose d'étudier l'effet des pannes optiques sur la qualité de service perçue directement par l'usager. Trois paramètres de qualité de service sont évalués : le taux de perte, le délai bout en bout et finalement la gigue des paquets. Ceci est d'une grande importance vu que c'est l'usager final du réseau qui éprouve les conséquences négatives des pannes. La simulation séparée des deux modèles permet de retrouver qualitativement les avantages et désavantages de chacun. Elle permet de regrouper les avantages de DiffServ* et DiffProtect. Une combinaison optimale permet d'avoir un maximum de performance en cas de pannes. Le chapitre 4 offre une étude plus élaborée sur certains aspects des modèles DiffServ* et DiffProtect, particulièrement leur coût de déploiement et la possibilité de leur utilisation dans des propositions de réseaux de future génération tel MPLS-DiffServ-TE.

Le deuxième objectif est de démontrer la faisabilité et de valider la performance du modèle DiffServ* en laboratoire. Cette étude fait l'objet du chapitre 5 du présent document.

Un désavantage de la méthode par simulation est son extensibilité et ses capacités de passage à l'échelle. Ceci amène au troisième et dernier objectif qui est étudié au chapitre 6 du projet et qui consiste à élaborer un modèle analytique de protection différenciée. Il permettra de retrouver pour toute taille de réseau, la combinaison DiffServ*/DiffProtect optimale qui garantit un maximum de performance en cas de panne et réduit à un strict

minimum les coûts associés au déploiement des mécanismes de protection optique.

1.2 Concepts de base

Les modèles de protection que nous avons proposés reposent sur l'utilisation de différents concepts :

- *le groupement de liens ou Link Bundling* est une technique qui permet l'agrégation de plusieurs canaux de communication pour former un seul conduit ou lien *logique* de plus grande capacité ;
- *le partage de charge ou Load Sharing* est, dans le cadre de ce projet, une conséquence directe du groupement de liens dans laquelle une certaine demande de trafic doit être divisée en plusieurs parties dont chacune est transmise sur un *lien composant ou Component Link* du groupement ;
- *le routage de connexion ou Connection Mapping* est le processus qui met en place les canaux de communication d'un groupement de liens sur un ou plusieurs chemins physiques ;

La figure 1.1 illustre l'application de ces trois concepts dans un réseau IP/WDM dans lequel la couche IP n'est autre que la couche logique du réseau et la technologie optique WDM représente la couche physique. Le lien logique entre les deux routeurs de la couche IP est un groupement de liens formé de trois composantes. Chaque lien composant correspond à une connexion donc un canal optique qui est mis en place sur un chemin physique qui relie le commutateur optique (OXC) du routeur source au OXC du routeur destination. Le flot de trafic du premier au deuxième routeur est divisé, par partage de charge, parmi les trois canaux optiques empruntables. Finalement, la capacité de transmission totale disponible à la couche IP entre les deux routeurs est égale à la somme des bandes passantes des trois canaux optiques composants qui le forment.

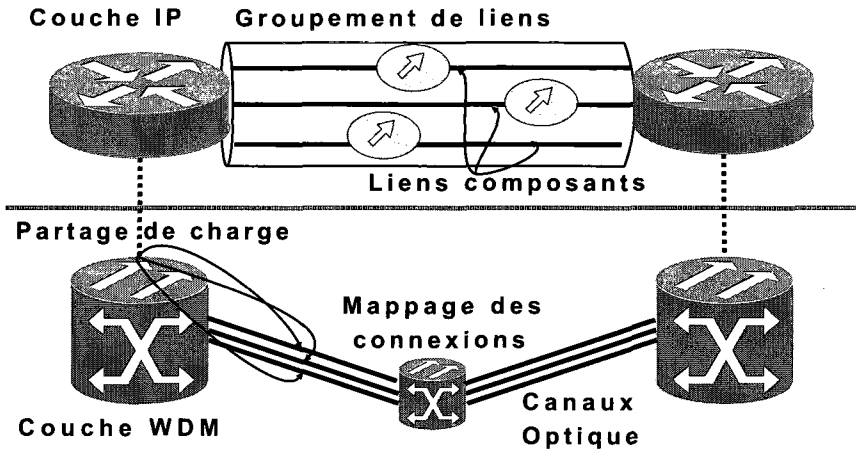


FIG. 1.1 Groupement de liens, partage de charge et routage de connexions IP/WDM

Dans tout réseau IP/WDM, la topologie virtuelle de la couche IP dépend grandement de l'utilisation des canaux optiques disponibles au niveau WDM physique. Un lien logique entre deux routeurs IP n'existe que s'il est possible d'établir une connexion tout optique de bout en bout entre ces deux routeurs. Du point de vue de la couche IP, cette demande de connexion se matérialise en un *canal optique* dédié à la transmission physique du trafic IP du lien en question. Du point de vue de la couche WDM, le canal optique est mis en place sur un chemin physique et devient *un chemin optique*. Il s'en suit alors que le trafic IP envoyé sur le lien considéré subit une conversion électrique-optique à la sortie du routeur, est transmis sur le chemin optique spécifié et subit une deuxième conversion optique-électrique à l'entrée du routeur destination.

Considérons le lien logique entre les routeurs A et B de la figure 1.2. Soit L la bande passante de ce lien. Pour établir un lien direct entre les routeurs A et B, il faut établir un ou plusieurs canaux entièrement optiques qui connectent les OXC sous-jacents 1 et 2. Le choix du chemin est facultatif et dépend uniquement du nombre de chemins physiques disponibles et de la capacité résiduelle de chaque chemin.

Soit $[1, 4, 2]$ le chemin physique considéré, la somme des bandes passantes des canaux optiques réservés sur ce chemin est de L. Tout le trafic IP routé sur le lien (A, B) devra

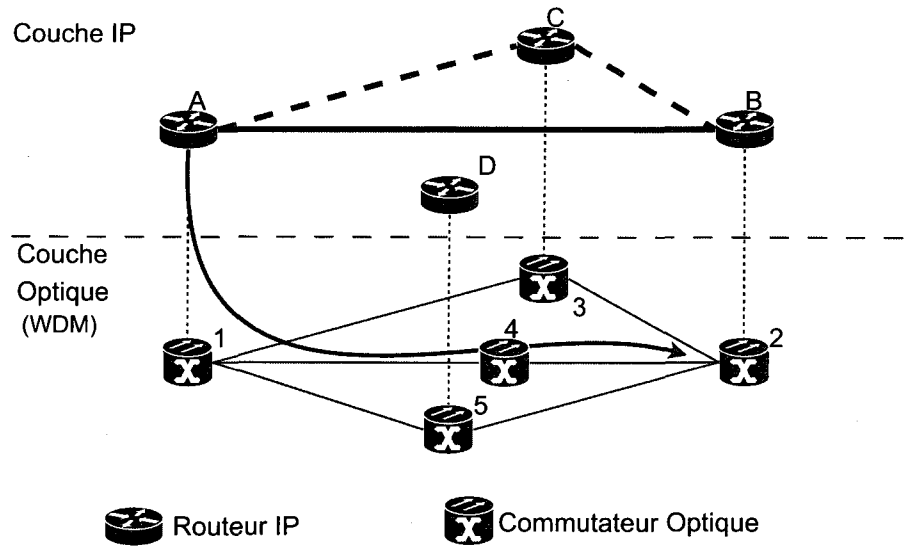


FIG. 1.2 Routage de connexion IP/WDM par chemin optique unique

transiter, après partage de charge et conversion optique, sur le chemin optique $[1, 4, 2]$. Si aucun mécanisme de protection optique n'est prévu et dès qu'il y a une panne sur le chemin $[1, 4, 2]$, le lien logique (A, B) tombe en panne à son tour, et tout le trafic IP entre les routeurs concernés sera perdu. Le flot de trafic IP doit compter sur les mécanismes lents de reroutage IP pour être rerouté sur un chemin secondaire, (A, C, B) par exemple, avant d'arriver à destination.

Considérons maintenant un *routage par séparation* dans lequel il est possible de réserver les canaux optiques d'un même lien logique sur plusieurs chemins différents. Si nous considérons le cas de la figure 1.3, il existe trois chemins disjoints reliant les commutateurs optiques 1 et 2. Les connexions requises par le lien logique (A, B) peuvent être routés sur les trois chemins disjoints disponibles. Nous aurons un canal optique de capacité $L/3$ sur chaque chemin.

Aucun changement significatif n'a eu lieu du point de vue de la couche IP. Que les trois canaux soient réservés sur un même chemin physique ou sur plusieurs, le résultat pour la couche logique est le même et la capacité de transmission totale disponible entre les

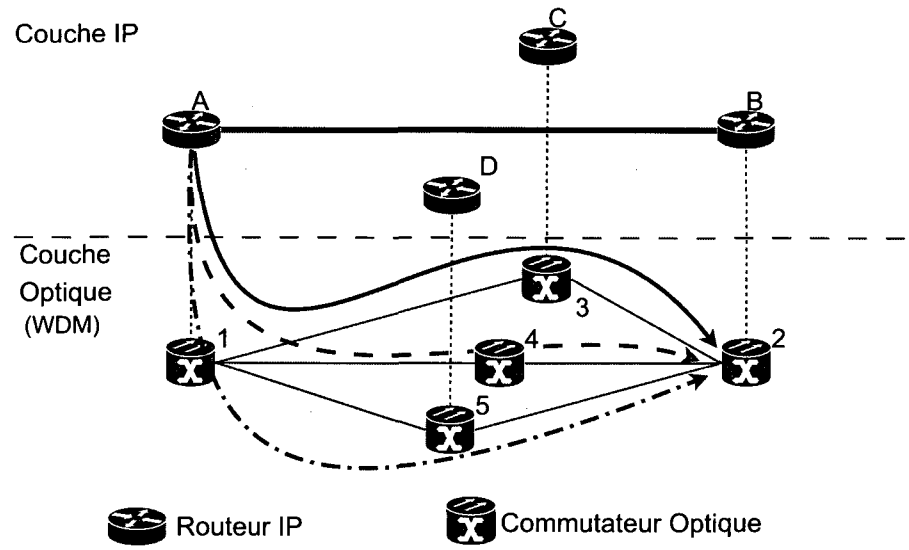


FIG. 1.3 Routage de connections optiques sur chemins multiples

routeurs A et B est toujours de L. La transmission du trafic de A vers B se fait sous forme entièrement optique, aucun routeur intermédiaire n'est sollicité dans cette communication.

Si un des trois chemins optiques tombe en panne, la connectivité logique entre les deux routeurs n'est pas entièrement perdue, mais seulement réduite. Comme une partie de la bande passante requise est réservée sur chaque chemin, si un des chemins tombe en panne, sa part de la capacité totale n'est plus disponible pour toute la durée de la panne. Dans ce cas, nous parlons d'une réduction de capacité entre les routeurs A et B et non plus d'une panne de lien logique entre ces noeuds.

L'avantage de cette option est qu'elle permet de retarder autant que possible les pannes des connexions et liens logiques. Il serait nécessaire que trois chemins physiques disjoints tombent simultanément en panne (phénomène très rare) pour avoir une panne du lien logique correspondant.

Le fait de pouvoir diviser le trafic d'un lien logique entre plusieurs canaux optiques disjoints permettrait de réduire l'effet ponctuel d'une panne physique. Cette idée est essen-

tielle puisqu'elle nous permettra d'offrir de la protection différenciée tant au niveau logique avec DiffServ*, qu'au niveau physique, avec DiffProtect. Les sections suivantes expliquent comment cette division peut être faite avec les technologies actuelles, et comment la protection différenciée serait assurée en cas de panne de chemins physiques.

1.2.1 Pratique et utilité du groupement de liens dans un réseau IP/WDM

Considérons l'exemple de deux routeurs A et B d'un réseau IP/WDM quelconque. Les routeurs sont adjacents, donc du point de vue IP, il existe un lien logique qui les relie. Si la demande de trafic entre les routeurs A et B est de 10Gb/s, la bande passante du lien (A, B) doit au minimum être égale à 10Gb/s. Pour rendre cette communication directe possible, il faut mettre en place un canal tout optique entre les routeurs A et B. La capacité de ce canal optique doit au minimum être égale à 10Gb/s.

Supposons que la demande de trafic sur le lien (A, B) augmente à 20Gb/s. La capacité du canal optique initial n'est plus suffisante pour accommoder la totalité de la demande de trafic entre A et B. La capacité du lien direct (A, B) doit être mise à jour ; plusieurs solutions existent.

La première solution est d'augmenter la capacité du canal optique déjà en place. Il faudra donc remplacer l'interface de transmission optique du routeur A par une autre de capacité supérieure. Selon (Widjaja and Elwalid, 2003), il n'est possible d'augmenter la capacité des interfaces de transmissions optiques que par un facteur de 4 (OC-3, OC-12, OC-48, OC-192,...). Il faudrait ainsi remplacer l'interface OC-192 de 10Gb/s par un système OC-768 de 40Gb/s pour accommoder 20Gb/s seulement. Selon (Sivarajan, 2000) la majorité des systèmes de transmission optique actuellement déployés sont capables de transmettre 10Gb/s sur chaque longueur d'onde et plusieurs efforts sont mis en oeuvre pour augmenter cette capacité à 40Gb/s. Cette augmentation est d'autant plus limitée en raison des effets de

dispersion de la lumière qui deviennent très significatifs quand le temps alloué à l'émission du bit est réduit.

L'autre solution est de mettre en place un autre canal optique de capacité 10Gb/s, parallèle au premier comme nous pouvons le voir à la figure 1.4. Cette technique est nettement préférable parce qu'elle permet une mise à jour plus graduelle de la capacité de transmission. Elle garantit ainsi un taux d'utilisation élevé des ressources de transmission. De plus, cette option reste plus économique que la première parce qu'elle requiert l'ajout d'une interface OC-192 de 10Gb/s plus courante et nettement moins coûteuse qu'une interface OC-768 de 40Gb/s.

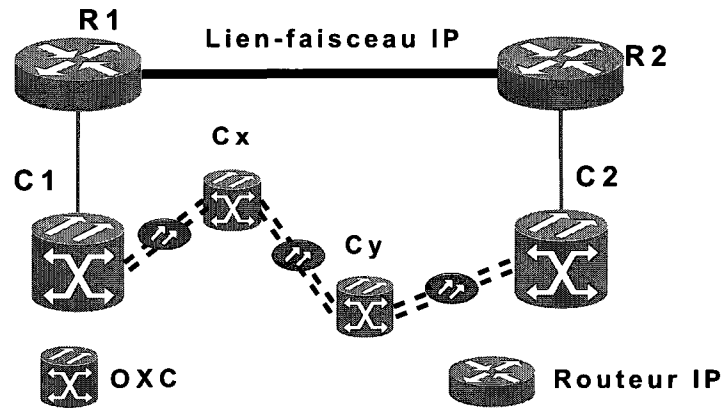


FIG. 1.4 Exemple d'un regroupement de liens IP/WDM

La figure 1.5 montre avec plus de détails un des routeurs de la paire (A, B) ainsi que le lien de 20Gb/s qui les relie. Deux canaux optiques de 10Gb/s chacun sont agrégés pour former le lien IP de capacité adéquate. Cette figure est inspirée de (Kimura et al., 2005) et montre aussi l'intérieur d'un noeud IP/WDM standard. Chacun des routeurs A et B est lié à un OXC, respectivement $C1$ et $C2$. Il existe deux chemins physiques disjoints entre les OXC $C1$ et $C2$. Le premier est direct $[C1, C2]$, l'autre possède un saut intermédiaire $[C1, C3, C2]$.

Dans le cas de la figure 1.5 et de la norme WDM, les deux canaux optiques agrégés

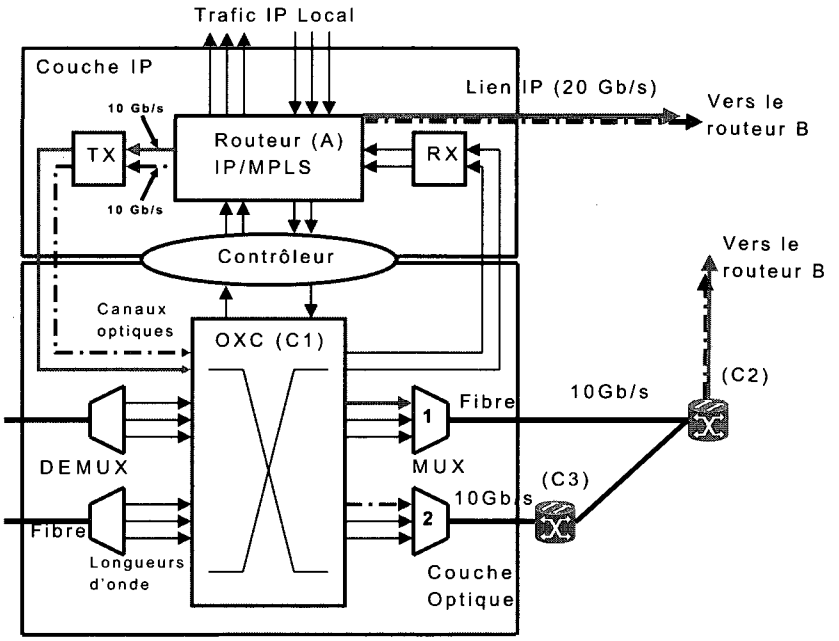


FIG. 1.5 Détails d'un noeud IP/WDM

forment alors un faisceau et le lien IP est un groupement de liens ou bien une connexion logique à :

- *Canaux multiples ou multi-channel ou bien à ;*
- *longueurs d'onde multiples ou multi-wavelength ou bien à ;*
- *chemins optiques multiples ou multi-lightpath.*

Ce lien possède un port de transmission logique associé à deux ports de transmissions physiques (*port-to-multiport trunk*). En ce qui concerne les mécanismes de routage IP tel OSPF, seules les caractéristiques du groupement de liens complet et non celles de chacune de ces composantes sont annoncées aux et par les routeurs. La technique de groupement de liens permet ainsi de réduire la quantité d'information échangée entre les routeurs et d'augmenter l'extensibilité (*Scalability*) du routage dans les réseaux IP/WDM. Ceci est mis en évidence dans (Sengupta et al., 2002) où les auteurs présentent une analyse d'une version améliorée de OSPF pour le routage de chemins optiques dans un réseau WDM.

Le routage des canaux optiques de la figure 1.5 est indépendant de la couche IP. Il est

possible que ces canaux soit multiplexés par le MUX 1 dans la fibre $[C1, C2]$ si elle possède deux longueurs d'onde inutilisées ou bien par le MUX 2, donc sur le chemin de fibres optiques $[C1, C3, C2]$, si la fibre $[C1, C2]$ ne possède pas les ressources nécessaires.

Quel que soit le chemin physique choisi, le flot de trafic entre les routeurs A et B devra être partagé entre les deux canaux réservés au niveau de couche optique. Il est alors évident que le partage de charge existe de façon naturelle dans un réseau IP/WDM. La charge de trafic d'un lien IP est partagée entre un ou plusieurs canaux de transmission optiques. Des contraintes de partage de charge par paquet ou par flot doivent toutefois être considérées pour assurer à la fois un partage équitable de la charge entre les deux canaux et une livraison ordonnée des paquets.

1.2.2 Problèmes liés au groupement de lien dans un réseau IP/WDM

Le groupement de liens permet de grouper plusieurs liens composants en un seul lien logique de grande capacité. Les protocoles de routage du niveau logique ignorent la présence des liens composants et ils annoncent et utilisent seulement les caractéristiques du groupement de lien logique final. Dans le cas d'un réseau IP/WDM, les liens composants sont des canaux optiques où chaque canal représente une longueur d'onde.

Le raisonnement de la section 1.2.1 montre que les longueurs d'onde sont généralement multiplexées sur un même chemin physique. Si un seul canal optique tombe en panne, la capacité du groupement de lien est réduite et des mécanismes de détection rapide sont déjà en place pour effectuer un nouveau partage de charge sur les liens composants fonctionnels. Dans le cas d'une coupure de fibre, tous les liens composants tombent en panne simultanément ; le lien logique correspondant tombe aussi en panne ce qui engendre un reroutage de plusieurs flots.

Le présent projet permet de contourner ce problème en forçant la réservation des canaux

optiques sur des chemins disjoints. Ceci est montré à la figure 1.5 dans laquelle un des canaux optiques est établi via le MUX 1 sur le lien direct $[C1, C2]$, le deuxième, via le MUX 2 sur le chemin $[C1, C3, C2]$. Cette opération est simple et une légère modification au contrôleur IP-WDM permet de réaliser cette tâche. D'ailleurs, s'il est possible de mettre en place les canaux optiques sur l'un ou l'autre des chemins, il est aussi possible de les séparer entre les deux chemins disponibles.

Cette pratique permet de rendre indépendantes les pannes des deux canaux optiques. La panne d'une fibre ne cause plus une interruption totale de la communication entre les deux routeurs, mais une réduction partielle du débit. Nous proposons ici de coupler cette version modifiée du groupement de liens, le partage de charge inhérent et l'architecture DiffServ pour former le modèle DiffServ* de la figure 1.6 et le modèle DiffProtect de la figure 1.10 qui, tous deux, fournissent une protection différenciée à plusieurs classes de trafic en cas de panne de fibre optique.

1.3 Les modèles de protection

Les deux modèles DiffServ* et DiffProtect se basent tous deux sur la division du trafic IP entre deux routeurs adjacents sur trois chemins physiques disjoints. Nous considérons pour l'instant que la division est égale et qu'elle nécessite un chemin optique par tranche de trafic. Les deux modèles considèrent trois priorités de trafic classifiées, d'après la section 2.1, comme suit.

Le trafic d'émulation de circuits ou de voix, classifié EF, possède la plus haute priorité ; il requiert des garanties très strictes en taux de perte, délai et gigue. Le trafic de vidéo est classé AF, il est de priorité moyenne en ce qui a trait à ses capacités de tolérance, de délais et de gigues. Le trafic Web qui caractérise généralement le trafic de transfert de fichiers, courriers électroniques et navigation Web est classé comme trafic de basse priorité (BE)

parce qu'il est le plus tolérant en termes de délais et de pertes.

1.3.1 Le modèle DiffServ*

Le modèle DiffServ* se base sur l'utilisation de l'architecture des services différenciés pour protéger les différentes classes de trafic contre les pannes physiques. L'architecture DiffServ offre trois classes de trafic principales EF, AF et BE. Un schéma fonctionnel du modèle DiffServ* est présenté à la figure 1.6. Ce modèle nécessite l'existence de trois chemins optiques physiquement disjoints pour communiquer entre deux routeurs adjacents, dans ce cas A (routeur source de trafic) et B (routeur destination de trafic). L'ensemble du trafic transmis par A est divisé en trois et chaque canal optique est utilisé pour transmettre une fraction mélangée des trois classes EF, AF et BE. Ainsi, la bande passante totale entre les deux routeurs est égale à la somme des bandes passantes des trois chemins physiques du niveau optique. Sachant que :

- plus le nombre de chemins optiques requis est grand, plus le lien IP est robuste face aux pannes mais ;
- plus le nombre de chemins disjoints requis est grand plus la probabilité d'en trouver dans un réseau IP/WDM maillé est faible.

Le choix du nombre de trois chemins optiques est ainsi un bon compromis entre la robustesse face aux pannes des liens logiques et la possibilité de trouver un nombre suffisant de chemins disjoints dans un réseau optique maillé.

Une panne sur un des chemins optiques entraîne une réduction des capacités de transmission au niveau WDM. Cette réduction est propagée au niveau IP, non comme une panne de lien logique, mais comme une réduction de la bande passante de ce dernier. Cette réduction de bande passante cause une congestion au niveau IP. Les mécanismes naturels de DiffServ de protection contre la congestion s'activent. Les trafics de hautes priorités obtiennent un accès privilégié aux ressources réduites du niveau physique. Les trafics de

basses priorités sont retardés et même rejetés jusqu'à réparation de la panne et restauration à l'état normal du service.

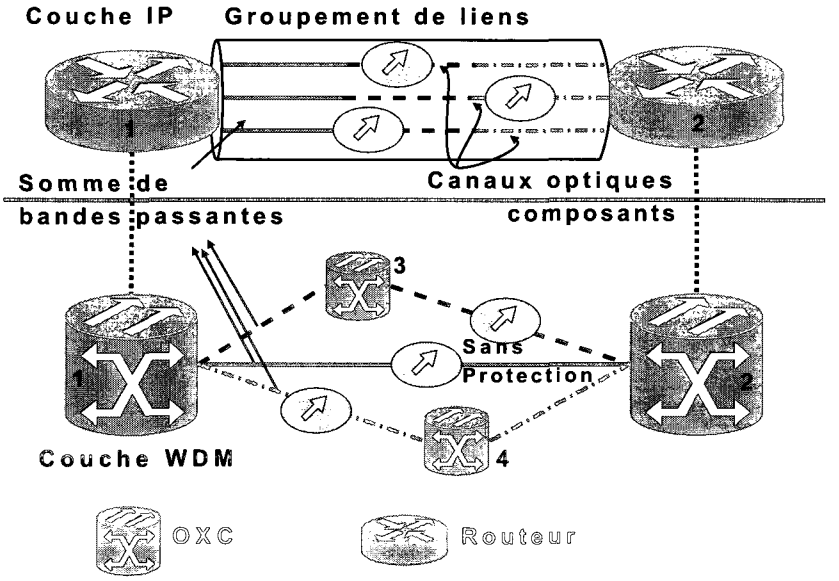


FIG. 1.6 Modèle DiffServ*

La figure 1.7 présente le fonctionnement détaillé d'un noeud source IP/WDM dans le cadre du modèle DiffServ*. Un classificateur DSCP se charge de détecter la classe de chaque paquet rentrant et de transférer chaque paquet dans la file appropriée au type des paquets IP qui arrivent au routeur. L'ordonnanceur DiffServ trie et transmet les paquets par ordre de priorité au modulateur électro-optique. L'information traverse un ordonnanceur électro-optique (OEOA) qui se charge de transmettre chaque paquet vers un des trois modulateurs. Chaque modulateur est associé à un canal optique réservé pour la transmission d'informations entre deux routeurs. Pour éviter tout désordre dans la réception des paquets, nous supposons que le partage de charge ci-dessus se fait de façon aléatoire par flot et non par paquet. Nous discutons des différences dans l'annexe I mais dans tout ce qui suit, nous voulons éviter tout problème de désordre de paquet qui peut être inhérent à la pratique de partage de charge en utilisant l'option par flot.

Le débit sortant du OEOA ne peut dépasser la somme des capacités des trois chemins optiques disponibles. Le débit de l'ordonnanceur DiffServ et la capacité du modulateur sont supposés égaux. Par phénomène de transition, le débit de l'ordonnanceur DiffServ ne peut dépasser la somme des capacités de transmission des trois chemins optiques. Toute surcharge de paquets au niveau du routeur IP est traitée comme une congestion par le module DiffServ. Le modèle DiffServ* proposé respecte le fonctionnement de l'architecture DiffServ et transmet de façon prioritaire la venue des paquets IP sur la capacité optique réservée.

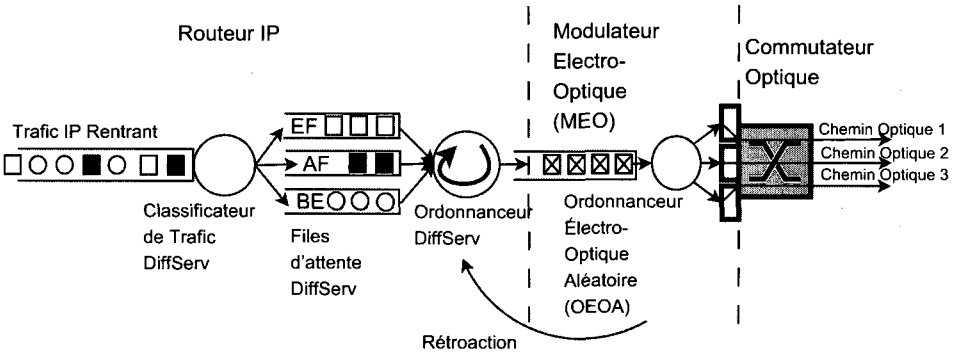


FIG. 1.7 DiffServ* : modulation et commutation optique du trafic IP

Dans le cas d'une panne d'un canal optique, sa capacité n'est plus disponible au niveau IP. Le modulateur optique se charge de détecter cette panne, et la communiquer à l'ordonnanceur DiffServ. Ce dernier se charge de réduire son débit d'information. Ce mécanisme de rétroaction garantit que la panne optique se propagera au niveau IP comme diminution de la bande passante.

Un dimensionnement adéquat des ressources optiques assure, en temps normal, une capacité de transmission suffisante pour toutes les connexions du niveau IP. Dans ce cas la bande passante des trois canaux optiques est juste suffisante pour garantir une qualité de service adéquate aux trois classes EF, AF et BE de trafic. La panne d'un des canaux optiques induit une congestion forcée au niveau du routeur IP. Le module DiffServ se charge

de transmettre de façon prioritaire les paquets IP sur les ressources réduites de la couche optique. Le modèle DiffServ* garantit toujours une distribution prioritaire de la capacité de transmission physique entre les différentes classes de trafic. La classe EF est la plus prioritaire et elle conserve donc un accès privilégié aux ressources physiques. Le trafic de la classe AF ne peut être servi qu'après celui de la classe EF. La classe BE est la moins prioritaire, le trafic de cette classe n'est servi qu'après EF et AF (service meilleur effort).

Un avantage immédiat du modèle DiffServ* est qu'il ne nécessite le déploiement d'aucun mécanisme de protection WDM. Les canaux optiques ne sont munis d'aucune protection particulière. Aucun reroutage optique n'est nécessaire dans le cas d'une panne. Une panne optique déclenche un mécanisme simple de rétroaction rapide, ce dernier spécifie au module DiffServ la diminution de bande passante impliquée, la protection des trafics de hautes priorités est quasiment instantanée. Un désavantage du modèle DiffServ* est qu'il ne permet aucune protection dans le cas d'une panne simultanée des trois chemins optiques. Dans ce cas très rare, la connectivité est totalement perdue entre les deux routeurs et un reroutage IP des flots est nécessaire.

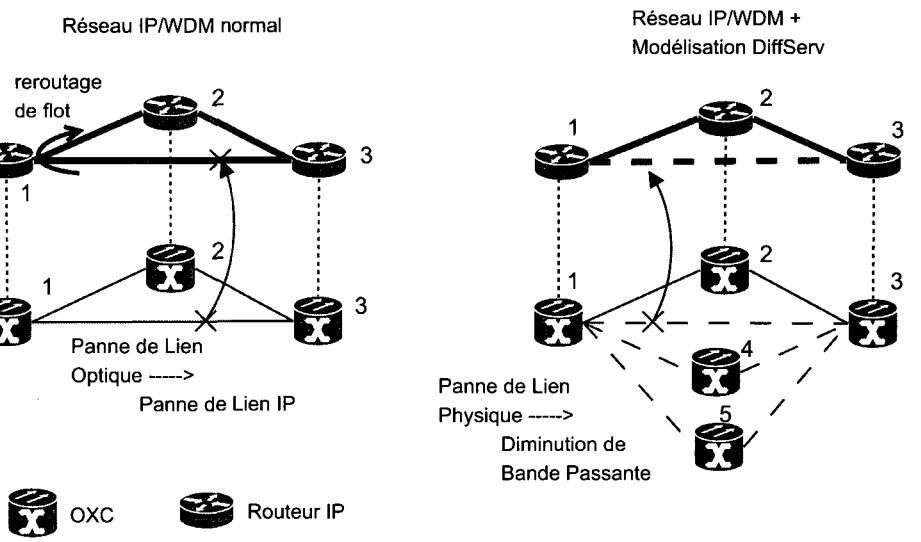


FIG. 1.8 Avantages du déploiement du modèle DiffServ*

La figure 1.8 compare l'effet d'une coupure de fibre optique dans un réseau IP/WDM à celle d'un réseau IP/WDM avec modélisation DiffServ*. Les deux réseaux ne sont munis d'aucune protection WDM particulière. Dans le premier cas, une panne du lien optique $[1,3]$ cause une panne du lien logique $(1,3)$. Le routeur 1 détecte la panne de lien, propage l'information à ses voisins, recalcule sa table de routage et reroute le flot $\{1,3\}$ sur le deuxième plus court chemin disponible $(1,2,3)$. La lenteur de ce mécanisme IP de reroutage peut causer une interruption de service inacceptable pour les trafics de hautes priorités. D'autant plus, le surplus non planifié de trafic sur le chemin $(1,2,3)$ peut causer une dégradation de performance accrue qui affecte autant le flot original du chemin que le flot rerouté. Le module DiffServ du routeur 1 doit à son tour protéger les trafics prioritaires de cette dégradation de performance.

Dans le deuxième cas, la panne du lien physique $[1,3]$ cause une simple diminution de bande passante au niveau du lien IP $(1,3)$. Aucune interruption de service n'a lieu, les flots de hautes priorités sont directement protégés par les mécanismes DiffServ. Le flot du chemin $(1,2,3)$ n'est pas affecté par cette panne. Si la panne du lien $[1,3]$ affecte de la même manière d'autres liens IP, le même argument tient toujours. Les conséquences d'une panne physique sont alors distribuées parmi plusieurs liens logiques, aucune interruption de service n'a lieu sur ces liens et l'architecture DiffServ garantit une qualité de service immédiate et appropriée aux flots prioritaires.

Grâce au modèle de protection DiffServ*, une augmentation de la demande de trafic sur un lien logique et la panne d'un ou plusieurs canaux de transmission physiques sous-jacents ont tous deux le même effet qui est la congestion comme nous pouvons le voir à la figure 1.9. Quelle que soit la nature du problème qui peut affecter le fonctionnement normal d'un noeud IP/WDM, le symptôme est toujours la congestion et le traitement est toujours DiffServ. Nous avons ainsi un mécanisme de protection unique qui peut distinguer facilement entre différentes classes de trafic et de les protéger adéquatement au besoin.

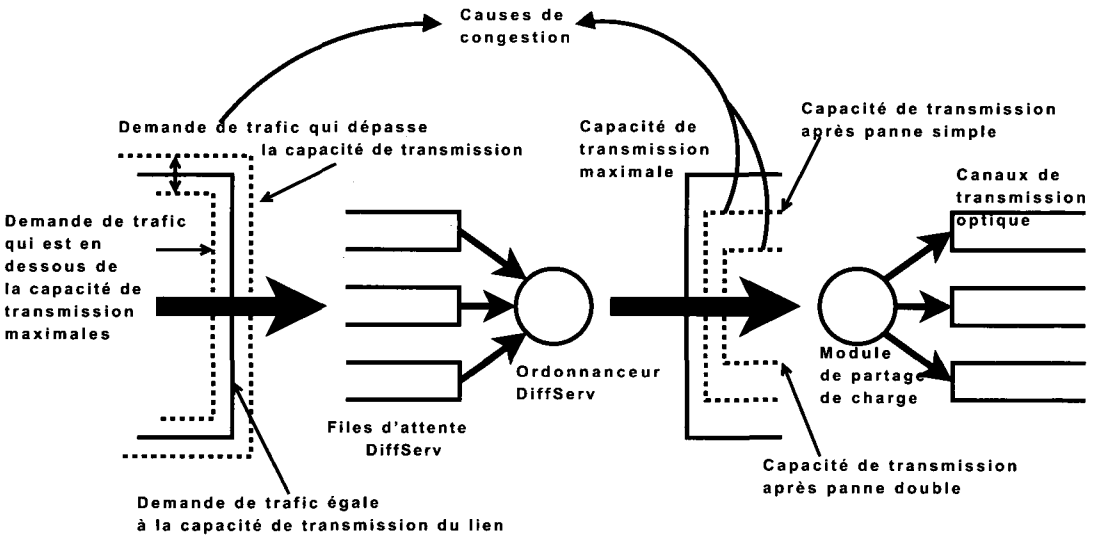


FIG. 1.9 Causes de congestion dans le modèle de protection DiffServ*

1.3.2 Protection de trafic dans DiffServ et DiffServ*

DiffServ a été conçu dans le but d'offrir une différenciation de service en cas de congestion dans un réseau IP. Il est seulement sensible à la congestion. Cette dernière a lieu quand la capacité des ressources de transmission n'est plus capable de supporter toute la charge de trafic. En cas de congestion, DiffServ est capable de privilégier certaines classes trafic et de les traiter de façon prioritaire. Ainsi, DiffServ se définit comme un mécanisme de *protection* différenciée *du trafic* contre le phénomène de congestion.

Généralement, le terme *protection* s'applique à la protection de circuits ou de canaux optiques où il s'agit de prévoir un canal de protection qui prend la relève en cas de panne du canal de transmission principal. Cependant, dans le cas de DiffServ, ce même terme indique l'action d'offrir une qualité de service (QdS) différenciée à différentes priorités de trafic en cas de congestion. Le modèle DiffServ* propose de réutiliser DiffServ et d'étendre ses fonctionnalités pour non seulement agir comme mécanisme de protection du trafic de haute priorité contre la congestion, mais aussi, contre les pannes du niveau de la couche de transmission, notamment la couche optique.

Il faut ainsi définir un moyen de traduire une panne optique en une augmentation de congestion, autrement dit, par une réduction de débit du serveur DiffServ. Cette réduction de débit cause une congestion à l'entrée du serveur DiffServ et les mécanismes naturels de DiffServ traiteront le trafic de façon prioritaire face à ce manque soudain en ressources de transmission.

Intuitivement, la solution serait de s'assurer que le trafic sortant du serveur DiffServ ne soit pas porté sur un seul système de transmission optique. S'il l'était, une panne de ce système n'apparaitrait pas comme une réduction de débit, mais simplement comme l'arrêt total du serveur. Il faut donc répartir le trafic sortant d'un serveur DiffServ sur plusieurs systèmes de transmission optiques. La panne d'un de ces systèmes de transmission n'implique pas un arrêt total du serveur, mais une diminution de sa capacité. Seuls les trafics de hautes priorités auront alors accès aux systèmes de transmission restants. DiffServ* devient ainsi un mécanisme de *protection* différenciée *du trafic* en cas de pannes de systèmes de transmission.

La réalisation du modèle DiffServ* ne peut se faire sans groupement de liens et sans partage de charge. Ce dernier se fait sur plusieurs canaux optiques. Si ces canaux sont multiplexés dans une même fibre, donc un groupement de liens traditionnel, DiffServ* protègera le trafic de haute priorité contre les pannes de canaux optiques seulement. S'il se fait sur des canaux optiques routés sur des fibres disjointes, DiffServ* protège contre les coupures de fibres aussi.

Ce projet doctoral vise principalement à déterminer l'efficacité de protection de l'architecture DiffServ en cas de panne d'un ou plusieurs liens composants d'un même groupement de liens. En temps normal, la capacité du serveur DiffServ est égale à la capacité du groupement de liens ; cette capacité est égale à la somme des capacités de ses groupements de liens. La panne d'un lien composant réduit la capacité du groupement de liens donc la capacité du serveur DiffServ aussi. Le serveur DiffServ se charge de protéger les tra-

fics de hautes priorités contre la congestion qui en résulte. Les pannes des *Component Links* deviennent indépendantes seulement quand ces derniers sont séparés sur plusieurs chemins disjoints. Seulement dans ce cas, DiffServ peut-il jouer le rôle d'un mécanisme de protection contre les pannes de chemins physiques dont les coupures de fibre pour un réseau WDM. Ceci constitue le modèle de protection différenciée DiffServ*.

1.3.3 Le modèle DiffProtect

Afin d'évaluer la protection offerte par le modèle DiffServ*, nous proposons un modèle similaire, DiffProtect. Ce dernier se base aussi sur la protection différenciée du trafic par des mécanismes propres à la couche physique. Pour procéder à une comparaison adéquate, il est nécessaire d'établir une base commune entre les deux modèles. Comme DiffServ*, DiffProtect doit aussi se baser sur le partage de charge du trafic sur trois canaux optiques disjoints pour respecter la condition d'indépendance des pannes des systèmes de transmission. Cependant, dans le cas de DiffProtect, ce partage de charge est différencié et se fait selon la classe et la priorité d'un flot. Il y a un seul type de trafic par lien composant et chacun est protégé différemment. La couche optique étant incapable de différencier entre les diverses classes de trafic, seule cette condition permet à DiffProtect d'offrir une protection physique faite sur mesure pour chaque classe.

À la différence du modèle DiffServ*, DiffProtect propose de transmettre chaque type de trafic sur un chemin optique qui lui est propre. Le modèle considère aussi trois priorités de trafic, EF, AF et BE. Un noeud IP/WDM-DiffProtect transmet le trafic de haute priorité sur un chemin muni d'une protection dédiée. Le trafic AF est de son côté transmis sur un chemin muni d'une protection partagée. Le trafic BE est transmis sur un chemin optique non protégé.

La figure 1.10 montre la topologie IP/WDM associée au modèle DiffProtect. La topologie

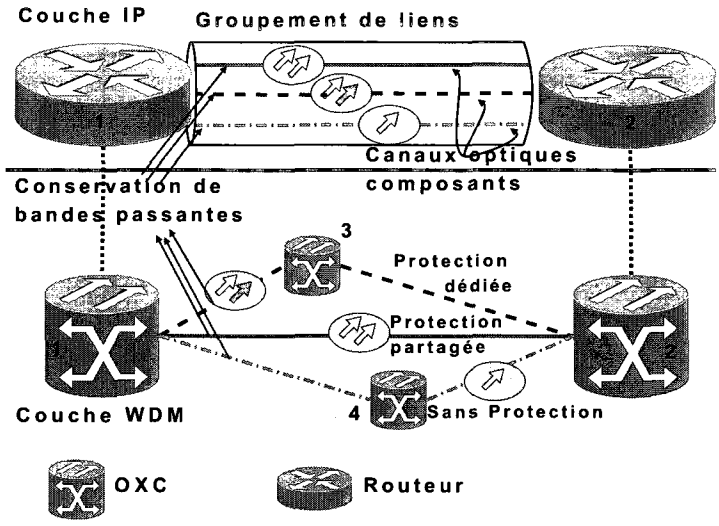


FIG. 1.10 Modèle DiffProtect

optique qui relie les deux routeurs IP est également constituée de trois chemins optiques disjoints, ce qui explique d'ailleurs le choix du nombre de trois chemins physiques considérés dans DiffServ*. Un même lien IP relie les routeurs 1 et 2. Cependant, les ressources du lien $(1, 2)$ ne sont pas partagés. Le lien IP $(1, 2)$ peut être vu comme une superposition de trois sous-liens : $EF(1, 2)$, $AF(1, 2)$ et $BE(1, 2)$. Dans ce cas, le protocole GMPLS peut être utilisé pour forcer le routage de chaque flot IP sur une longueur d'onde qui lui est propre. Pour cette topologie, le trafic de haute priorité est transmis sur le chemin optique protégé $[1, 2]$. Le chemin partiellement protégé $[1, 3, 2]$ transporte le trafic de moyenne priorité. Le chemin non protégé $[1, 4, 2]$ transporte le trafic de basse priorité.

La figure 1.11 montre le détail de la modulation IP-optique du trafic lors de sa transmission par la couche physique. Suite à une étape de préclassification du trafic entrant au routeur, chaque paquet sera acheminé vers le port de sortie adéquat selon sa classe. Chaque classe de trafic traverse son propre système de file d'attente FIFO avant de subir la modulation IP-optique. Le débit du serveur FIFO de chaque classe ne peut dépasser la capacité du canal optique spécifié.

Dans le cas de pannes du chemin principal $[1, 2]$, l'OXC se charge de commuter le trafic

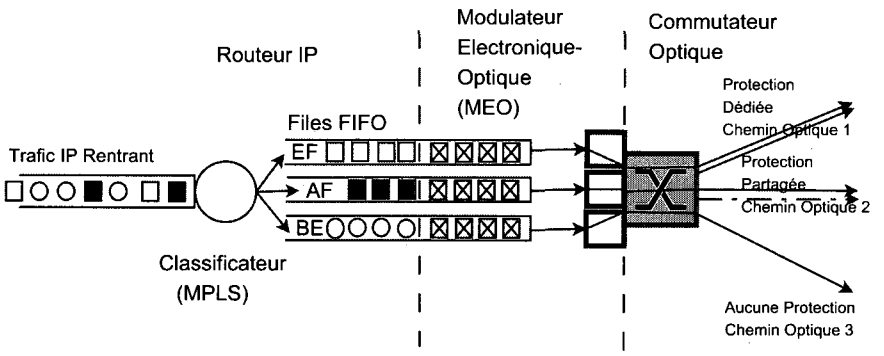


FIG. 1.11 DiffProtect : modulation et commutation optique du trafic IP

EF sur le chemin de protection. Pour la technologie WDM, l'interruption de service dure environs 50 ms et ne présente aucun effet détectable sur la qualité de service offerte au trafic EF. À toute fin pratique, le lien $EF(1,2)$ n'est pas affecté par la panne.

Seule une panne du chemin $[1,3,2]$ peut affecter le flot AF. Dans ce cas, le trafic AF ne garantit qu'une protection partielle. Seule une portion α du trafic est reroutée sur le chemin de protection. La bande passante réduite du lien de protection cause une accumulation de trafic dans la file FIFO du lien $AF(1,2)$. Les rejets de paquets se font à ce niveau. Seule une panne du chemin $[1,4,2]$ peut affecter le trafic BE. Comme ce chemin n'est muni d'aucune protection, tout le trafic BE sera perdu jusqu'à réparation de la panne.

Un avantage évident du modèle DiffProtect est que même dans le cas d'une panne simultanée des trois chemins optiques, la connectivité est toujours maintenue pour les classes EF et AF. Le déploiement des mécanismes de protection WDM même s'ils sont plus coûteux, garantit dans tous les cas une protection totale du trafic hautement prioritaire et une protection partielle du trafic de moyenne priorité, ceci est à condition que les chemins de protection d'EF et AF soient disjoints des trois chemins optiques originaux utilisés pour transmettre le trafic en temps normal.

DiffProtect peut paraitre très exigeant en terme d'utilisation des ressources physiques

puisqu'il nécessite un minimum de cinq canaux optiques qui soient physiquement disjoints. Trois de ces canaux sont utilisés pour la transmission du trafic en mode normal et deux sont réservés pour la protection dédiée et partagée du trafic prioritaire en cas de pannes. Bien qu'il puisse exister des solutions de protection optique plus efficace en terme d'utilisation de ressources, DiffProtect demeure plus robuste face aux pannes multiples. La section 4.2 décrit en détail ce point de vue.

CHAPITRE 2

REVUE DE LITTÉRATURE

Une recherche bibliographique approfondie a été réalisée dans le but de démontrer la pertinence et l'originalité du présent projet doctoral. La section 2.1 montre un consensus général dans l'utilisation de l'architecture DiffServ comme mécanisme de choix pour garantir une qualité de service différenciée dans le réseau Internet. La littérature n'offre qu'une description qualitative et quantitative de l'utilisation et du déploiement de l'architecture DiffServ comme mécanisme de contrôle et de protection contre la congestion au niveau IP ; elle ne semble proposer aucun autre usage de cette architecture. Ceci dévoile déjà une facette originale du projet. Cette dernière consiste en une utilisation duale de Diffserv comme mécanisme de protection contre la congestion et contre les pannes du niveau physique.

Seule la technologie WDM peut exploiter au maximum les capacités de transfert considérables des fibres optiques. Par multiplexage de longueurs d'onde, une fibre optique est capable de transporter plusieurs gigabits et même terabits par seconde d'informations. Par contre, une panne de fibre engendre une perte aussi considérable en données. Ceci justifie davantage la nécessité de déployer des mécanismes de protection physique rapides et fiables pour contrer les pannes du niveau optique. Cependant, plusieurs contraintes peuvent s'opposer au déploiement à large échelle de ces types de mécanismes. La section 2.2 montre les défis, avantages et inconvénients associés à l'utilisation de la protection optique. Des alternatives offertes par d'autres couches en sont subséquemment explorées. Les divers mécanismes de protection différenciée sont explorés en détail dans la section 2.3. Le but de cette étude est principalement de montrer la popularité et la pertinence de la notion de fiabilité différenciée dans les réseaux IP/WDM, mais aussi de mettre

en valeur l'originalité de ce projet par rapport à ce qui est déjà proposé.

2.1 L'architecture DiffServ

Cette section a pour but de décrire l'architecture des services différenciés (DiffServ) (Blake et al., 1998; Heinanen et al., 1999; Jacobson et al., 1999; Nichols et al., 1999), de préciser les diverses techniques de déploiement de cette architecture dans les réseaux IP/WDM actuels et finalement de présenter un rapport détaillé des évaluations de performance qualitatives et quantitatives de cette dernière. L'association type trafic/classe DiffServ est élaborée à la fin de cette section.

2.1.1 Description de DiffServ et fonctionnement général

La nature meilleur effort du réseau Internet le rend simplement incapable d'offrir un niveau de QdS approprié aux diverses applications multimédias temps réel qui l'utilisent. L'architecture DiffServ (Blake et al., 1998) a été proposée dans le but d'offrir une qualité de service différenciée à diverses classes de trafic du réseau Internet.

IntServ (Integrated Services) (Braden et al., 1994) a déjà envisagé le problème de différenciation de service. Il utilise le concept de réservation de ressources par le biais du protocole Ressource reSerVation Protocol (RSVP) pour garantir une qualité de service adéquate à chaque flot séparément. IntServ recommande une réservation de bout en bout pour chaque flot, ce qui augmente considérablement le trafic de signalisation nécessaire à ce processus. Les concepteurs ont rapidement réalisé les problèmes de complexité, extensibilité, et coûts de déploiement à large échelle de l'architecture IntServ. Ces incidences s'expliquent par le fait que chaque routeur devra gérer simultanément plusieurs milliers et mêmes millions de connexions (Nguyen et al., 2000), rendant l'architecture IntServ très

peu extensible et adaptable à toute taille de réseau.

Devant de tels désavantages à l'utilisation de IntServ, DiffServ a été élaboré. Ce dernier délaisse toute notion de réservation de ressource et de signalisation. Pour remplacer et améliorer celle-ci, DiffServ fait en sorte que les flots de trafic qui requièrent des garanties de services similaires soient regroupés ensemble. Pour ce faire, les routeurs de bords (EDGE) du réseau se chargent de classifier et marquer les paquets entrants. Chaque paquet est marqué par un DSCP (DiffServ Code Point) qui identifie sa classe de service. Les routeurs de coeur (CORE) du réseau se chargent d'acheminer chaque paquet en respectant sa priorité. Un comportement par saut (Per-Hop Behavior ou PHB) est associé à chaque classe de trafic. Par conséquent, un accès privilégié aux ressources sera réservé aux paquets de haute priorité et ce sont les paquets de plus basses priorités qui seront les plus sujets aux délais élevés et aux rejets en cas de congestion.

Pour différencier les trafics, DiffServ les divise principalement en trois classes. D'une part, nous avons la classe Expedited Forwarding (EF) (Jacobson et al., 1999) dont le niveau de priorité est le plus grand. Pour cette classe, le taux de pertes des données, les délais et les gigues sont les plus petits. D'autre part, nous avons la classe AF (Assured Forwarding) (Heinanen et al., 1999). Les paquets de moyenne priorité sont associés à cette classe. Cette dernière comporte quatre sous-classes. Une sous-classe AF est identifiée par $AFxy$ dans laquelle x représente la sous-classe AF, $1 \leq x \leq 4$. y représente la priorité de rejet du paquet, $1 \leq y \leq 3$. Chaque sous-classe peut être configurée pour offrir jusqu'à trois priorités de rejet. Une fois que la classe x d'un paquet est déterminée, le routeur EDGE se base sur une politique de marquage, Token Bucket, srTCM (Heinanen and Guerin, 1999a) ou trTCM (Heinanen and Guerin, 1999b) pour déterminer la priorité de rejet d'un paquet.

Chaque politique de marquage définit un profil particulier pour chaque classe de trafic. Les paquets qui respectent le profil défini seront plus prioritaires que ceux qui respectent moins ou pas ce même profil. Pour se faire, srTCM mesure le débit de trafic entrant contre

deux valeurs, la première, le CBS (Commited Burst Size) et la seconde, EBS (Excess Burst Size). Un paquet est marqué vert s'il respect la limite CBS, jaune s'il ne respecte pas le CBS mais l'EBS, et rouge s'il ne respecte pas l'EBS. Pour la classe AFx, les paquets verts seront les plus prioritaires, ils appartiennent à la classe AFx1, Les paquets jaunes, de moyenne priorité feront partie de la sous-classe AFx2 et les paquets rouges seront les premiers paquets de AFx à être rejetés en cas de congestion, ils ont la priorité de rejet, AFx3.

Le diagramme de la figure 2.1 présente une récapitulation des fonctionnalités EDGE et CORE d'un noeud DiffServ. Selon cette figure, un routeur EDGE a la responsabilité de classifier et marquer un paquet selon sa nature et son respect d'un profil de trafic prédéfini. Un DSCP est attribué à chaque paquet à la sortie du module de classification d'un EDGE.

Un noeud CORE comporte plusieurs files d'attente physiques. Une file d'attente est attribuée à chaque classe EF, AFx et BE. Les files physiques AFx sont divisées en y files virtuelles. Ces dernières sont généralement de type Random Early Detection (RED). Contrairement aux files de types First In First Out (FIFO), les files RED ont la capacité de rejeter les paquets de façon probabiliste avant que la taille maximum de la file d'attente ne soit atteinte. Une file RED accepte tout paquet entrant tant que sa taille est inférieure à une certaine limite Minimum Threshold (MinTh). Si la taille de la file RED est supérieure au Maximum Threshold (MaxTh), tout paquet rentrant est rejeté. Finalement, si la taille de la file est supérieure au MinTh mais inférieure au MaxTh, les paquets sont rejetés avec une probabilité qui varie en fonction de la taille de la file. Ces calculs probabilistes de rejet sont fonction du type de files RED. En effet, il existe quatre types de files RED : RIO-C, RIO-D, DROP et WRED.

Dans un noeud CORE, les files d'attente sont servies selon un ordonnancement qui peut être prioritaire (PRI), Weighted Round Robin (WRR), Weighted Interleaved Round Robin (WIRR) et Round Robin tout court (RR). Dans PRI, les files sont servies par ordre de

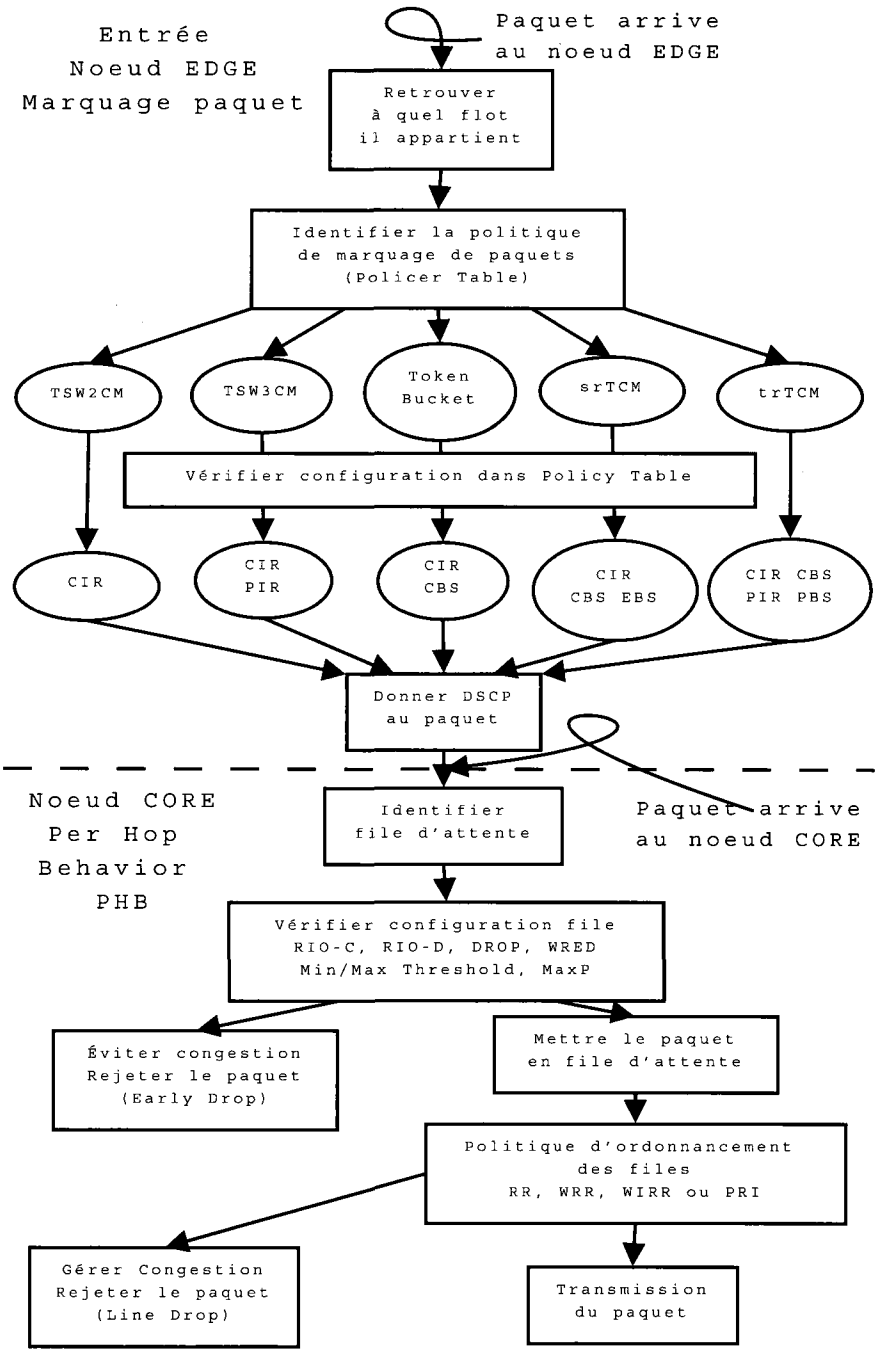


FIG. 2.1 Diagramme des fonctionnalités EDGE ou CORE de DiffServ

priorité. Il faut complètement servir les files de haute priorité avant de servir celles de basses priorités. WRR et WIRR affectent des poids aux files. Pour un intervalle de temps donné, la file qui possède le poids le plus élevé est servie pendant une fraction de temps plus élevée. Dans RR, les files ont toutes la même priorité et sont servies à tour de rôle. Dans ce cas, la notion de priorité de service disparait.

2.1.2 DiffServ dans un réseau IP/WDM

Selon (Kimura et al., 2005), il existe deux méthodes de différenciation de trafic dans un réseau IP-Optique. La première est basée sur le concept de DiffServ. Les auteurs y réfèrent par le terme de Class-Based Queueing (CBQ). Le fonctionnement de l'architecture CBQ est schématisé dans la partie supérieure de la figure 2.2 qui est tirée de (Kimura et al., 2005). Un chemin optique λ est utilisé pour servir les différentes classes de trafic EF, AF et BE. Deux systèmes de files d'attente CBQ, l'un d'entrée du routeur, l'autre de sortie, assurent un traitement PHB prioritaire et différencié des paquets. Un commutateur de paquets assure la transition correcte des paquets entre le port d'entrée et celui de sortie. Le débit des paquets au port de sortie doit être inférieur ou égal à la capacité d'une longueur d'onde. Si ce débit est supérieur au taux de conversion optoélectrique, les paquets devront être rejetés par ordre de priorité dans le système CBQ de sortie.

L'autre option proposée par les auteurs est d'ajouter une deuxième longueur d'onde au niveau du même port de sortie. La partie inférieure de la figue 2.2 montre la deuxième méthode proposée : la Class-Based Lightpath (CBλ). Cette méthode suggère de transmettre chaque classe de trafic sur une longueur d'onde qui lui est propre. S'il existe trois classes de trafic au niveau IP (EF, AF et BE), chaque lien IP nécessitera au minimum trois chemins optiques au niveau WDM. Une conversion optoélectrique indépendante se fait pour chaque type de trafic à l'entrée du routeur. Une file de types FIFO est nécessaire pour chaque chemin optique. Dans ce cas, le débit d'une classe de trafic ne doit pas dé-

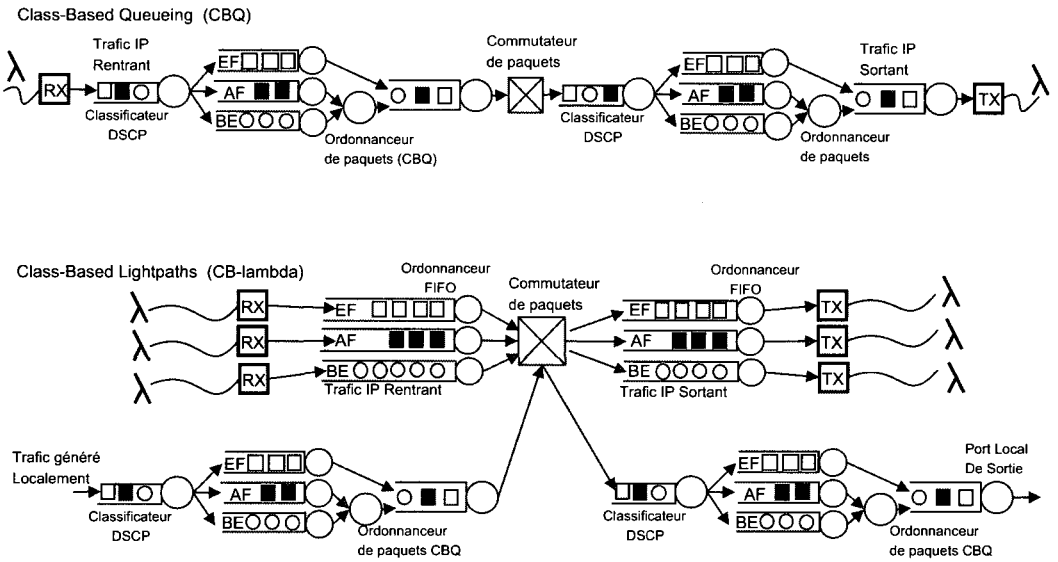


FIG. 2.2 Différenciation de trafic dans un réseau IP/WDM

passer la capacité de transmission d'une longueur d'onde. Une deuxième longueur d'onde doit être réservée par trafic excédentaire. Dans ce deuxième modèle, seul le trafic généré localement par le routeur IP ou qui quitte le routeur passe par un système de files CBQ. Le trafic de transit utilise des files FIFO. Le conditionnement et la différenciation de service se font uniquement aux extrémités d'un chemin IP. Un dimensionnement adéquat à l'intérieur du réseau garantit la disponibilité des ressources aux diverses classes de trafic.

Les auteurs citent deux types de transmissions dans un réseau IP/WDM :

- **Saut-par-Saut IP** : L'information qui traverse un noeud IP/WDM subit obligatoirement une conversion optoélectrique. Cette méthode est à la fois extensible et diminue le nombre de chemins optiques nécessaires pour les transmissions, car elle permet l'agrégation des flots de données au niveau IP pour être transmise sur une même longueur d'onde au niveau optique.
- λ **cut-through transmission** : L'information qui traverse un noeud IP/WDM peut ne subir aucune conversion optoélectrique. Cette méthode permet d'éviter la nécessité des algorithmes de routage IP complexes dans les noeuds intermédiaires, simplifiant consi-

dérablement leur structure.

Kimura et al terminent en proposant et en comparant les coûts des quatre modèles de qualité de service suivants :

- Saut-par-Saut IP et modèle CBQ
- Saut-par-Saut IP et modèle CBλ
- λ cut-through transmission et modèle CBQ
- λ cut-through transmission et modèle CBλ

Le concept de protection différenciée contre les pannes n'est pas étudié par les auteurs. Le modèle de protection DiffServ* proposé par ce projet doctoral reprend l'idée du modèle CQB de (Kimura et al., 2005) mais nécessite la division obligatoire du trafic d'un lien entre un minimum de trois chemins optiques. La panne d'un chemin optique entraîne une congestion du port de sortie permettant à DiffServ* d'assurer une protection différenciée en cas de panne.

Le modèle DiffProtect reprend l'idée du modèle CBλ de (Kimura et al., 2005). Chaque type de trafic est transmis sur une longueur d'onde qui lui est propre. La couche optique assurera une protection prioritaire du trafic en cas de panne de chemin optique. Le chemin optique réservé pour le transport du trafic EF sera muni d'une protection dédiée. Un chemin de protection partagé sera fourni au chemin qui transporte le trafic de moyenne priorité. Aucune protection n'est fournie au trafic de basse priorité. Les concepts de transmission Saut-par-Saut IP et de λ cut-through sont aussi envisagés par le présent projet. Le modèle DiffServ* suppose une transmission tout optique entre deux routeurs IP. DiffProtect nécessite une conversion optoélectrique de l'information à certains endroits du réseau. L'étude menée par (Kimura et al., 2005) ne combine pas l'utilisation simultanée des modèles CBQ et CBλ dans un même réseau mais peut être adaptée à l'évaluation des coûts associés au déploiement des mécanismes de protection DiffServ* et DiffProtect dans un réseau IP/WDM.

2.1.3 DiffServ dans la littérature

La performance de l'architecture DiffServ est analysée en profondeur dans plusieurs travaux. La popularité croissante de DiffServ dans la littérature démontre son utilisation grandissante dans le réseau Internet de prochaine génération. Plusieurs études sont consacrées à l'évaluation de performance de l'architecture DiffServ dans les réseaux IP. Leur but est de raffiner la configuration des routeurs DiffServ pour maximiser la performance et la protection des trafics de hautes priorités. La différence essentielle entre ce projet et tout ce qui est présenté dans la littérature est que nous proposons l'utilisation de DiffServ non seulement comme mécanisme de protection contre la congestion des routeurs IP mais aussi comme mécanisme de protection logique et immédiat contre les pannes du niveau optique. L'utilisation de DiffServ devient alors double. Elle protège toujours les flots contre la congestion à l'entrée et à la sortie d'un routeur DiffServ, mais aussi contre les pannes des niveaux inférieurs.

Les travaux de (May et al., 1999) sont inspirés par le fait que l'architecture des services différenciés se base sur le concept de marquage des paquets IP. Un concept simple, facilement implantable et extensible. Ce marquage permet d'offrir un service spécifique à chaque classe de paquets. Les auteurs recherchent des expressions simples pour quantifier le service offert aux paquets marqués, non marqués et la fraction des paquets marqués qui ne reçoivent pas la performance voulue. Ils ont obtenu des expressions pour évaluer la performance des classes Premium Service Scheme et Assured Service Scheme, équivalents respectifs de l'appellation courante connue des classes EF et AF. Cette étude pourra leur permettre d'établir de façon simple une différenciation de tarif entre les services offerts : un tarif spécifique par classe de service. Pour pouvoir garantir un taux de transfert minimal aux applications, la classe AF doit définir un profil de service. Le trafic AF doit se conformer à ce profil. Les paquets conformes (In-Profile) sont donc marqués 1. Les paquets non conformes (Out-of-Profile) ne sont pas marqués. Un profilomètre (Profile

Meter) permettant d'accomplir cette tâche peut être, par exemple, le leaky bucket filter.

May el al. citent trois méthodes pour rejeter les paquets conformes ou non. D'une part, dès que la taille de la file d'attente atteint un certain niveau M, seuls les paquets non conformes sont rejetés dès que M est atteinte. Un autre moyen est d'utiliser l'extension de RED, le RIO (RED with In and Out packets) qui permet de gérer simultanément deux services, celui des paquets conformes versus non conformes. Le système offre un seuil de rejet différent pour chaque type de paquets. Le seuil de rejet des paquets non conformes est inférieur à celui des paquets conformes. Enfin, le troisième moyen consiste à faire en sorte qu'un paquet conforme soit admis dans une file d'attente pleine s'il y a au moins un paquet non conforme déjà dans la file. Un paquet non conforme est rejeté de la file pour faire place au paquet conforme qui vient d'arriver. Les auteurs suggèrent qu'il est possible d'obtenir des garanties de service déterministes, même pour les paquets marqués.

Le Premium Service Scheme alloue une bande passante spécifique aux trafics de hautes priorités. Le service doit spécifier un débit crête et une taille maximum de rafale pour les flots concernés. Les flots ne peuvent dépasser les limites spécifiées. En retour, le réseau garantit la qualité de service offerte aux paquets de cette classe. Les routeurs du réseau garantissent un traitement immédiat aux paquets Premium, les paquets Best Effort sont mis en attente tant qu'il y a toujours des paquets de haute priorité à servir. Deux modèles analytiques simples sont subséquemment proposés. Le premier caractérise le Assured Service Scheme, l'autre, le Premium Service Scheme. Les modèles permettent, par exemple, de déterminer la taille des files ainsi que les fonctions de rejets d'une file nécessaires pour garantir un débit minimal aux applications de la classe AF. Les modèles ont permis aux auteurs de déterminer les principaux paramètres qui affectent la performance du réseau, par exemple, les paramètres des files RIO.

Les auteurs de (Sahu et al., 1999) analysent deux problèmes clés de l'architecture Diff-Serv. Dans le premier, il s'agit de déterminer la façon avec laquelle un routeur doit traiter

les paquets des différentes classes. Dans le deuxième, il s'agit de savoir si un routeur EDGE doit rejeter un paquet qui ne respecte pas le profil de trafic défini (Edge-Dropping) au lieu de le transmettre avec une priorité de rejet plus élevée (Edge-Marking).

Pour ce qui est du traitement des paquets, une option est de munir un routeur de plusieurs files FIFO, une par classe de service, qui sont servies suivant un ordonnancement prioritaire (priority scheduling). Une autre option serait de permettre aux différentes classes de services de partager une même file d'attente. Le routeur associe à chaque classe un seuil de rejet. Les paquets d'une classe ne sont rejetés que si le seuil de rejet de cette classe est atteint (Threshold Droping). En ce qui concerne le deuxième problème, Sahu et al. citent plusieurs références qui montrent que l'option Edge-Marking permet d'améliorer le taux d'utilisation des ressources du réseau. Les conséquences de cette option sur certains protocoles spécifiques, tel TCP, restent cependant inconnues. Les auteurs étudient délai et taux de pertes du réseau en dérivant des modèles analytiques qui combinent priority scheduling, Threshold Droping, Edge-Marking et Edge-Dropping. Les résultats montrent que le priority scheduling est plus efficace que le Threshold Droping en termes de délai mais moins efficace en termes de taux de perte quand des sources de trafic en grandes rafales sont utilisées. Le Edge-Marking améliore le débit des connexions TCP seulement quand la source TCP choisit soigneusement la quantité de paquets non conformes transmis dans le réseau.

Une extension des travaux de (May et al., 1999) et (Sahu et al., 1999) est réalisée dans (Nguyen et al., 2000). Les auteurs présentent une approche analytique qui permet d'évaluer la performance d'une file d'attente à N seuils de rejet, comparativement à deux seuils de rejet de (May et al., 1999) et (Sahu et al., 1999)). Ce mécanisme est celui proposé pour la classe AF. Nguyen et al. utilisent des modèles de trafic poisson avec des temps de service exponentiels. Les auteurs montrent aussi que même si une source de trafic poisson ne peut modéliser adéquatement une source de trafic en rafales, le modèle poisson demeure valable pour une agrégation d'un grand nombre de telles sources.

Les travaux de (May et al., 1999), (Sahu et al., 1999) et (Nguyen et al., 2000) montrent la complexité impliquée dans la modélisation analytique et adéquate du fonctionnement d'un noeud DiffServ. Une alternative à la modélisation analytique est d'utiliser une approche statistique pour caractériser la QdS offerte à différentes classes de trafic. Les auteurs de (El-Gendy et al., 2003) présentent un PHB comme étant l'élément principal d'un domaine DiffServ. Un PHB est spécifié pour la classe EF, un autre pour la classe AF. La concaténation de plusieurs PHB (EF ou AF) peut refléter la qualité de service de bout en bout offerte à une classe de trafic par le réseau. Le délai, la gigue, le taux de perte et le débit d'un trafic sont les paramètres qui mesurent la qualité de service d'un PHB. Cette qualité de service dépend intrinsèquement de la configuration minutieuse des paramètres de files d'attente, de gestion des tampons, de l'ordonnancement, des policer et des filtres de trafic. Gendy et al. évaluent par analyse factorielle l'effet de différentes configurations de PHB avec plusieurs scénarios de trafic donnés. Ils utilisent ANOVA (ANalysis Of VAriance) pour identifier les données et les paramètres qui influencent le plus la performance d'un PHB. Ils utilisent ensuite une analyse par régression multiple pour modéliser la QdS d'un PHB en fonction de ces paramètres.

Nous avons trouvé plusieurs autres références qui caractérisent analytiquement la différenciation de service basée sur l'architecture DiffServ. Un White Paper qui détaille l'implémentation de DiffServ dans des grands réseaux IP est présenté dans (Semeria and Stewart III, 2001) où les auteurs discutent l'effet du multiplexage statistique des paquets sur la qualité de service du réseau. Les paramètres de qualité de service considérés sont le débit, le taux de perte, le délai et la gigue. Les travaux de (Wydrowski et al., 2002) proposent de modéliser deux classes de services, une classe de haute priorité A qui regroupe les trafics de voix et vidéo. L'autre, B, regroupe le trafic TCP, FTP et HTTP et les classifie comme meilleur effort. Wydrwoski et al. considèrent un ordonnanceur prioritaire qui transmet les paquets de la classe A avant ceux de la classe B. DiffServ ne prévoit aucun mécanisme de signalisation et de contrôle de flot. Un dimensionnement et une planifica-

tion de capacité deviennent alors impératifs dans un réseau DiffServ. Les auteurs de (Wu and Reeves, 2003) et (Wu. and Reeves, 2004) formulent un problème qui minimise le coût des liens d'un réseau DiffServ en fonction de la qualité de service offerte à uniquement deux classes : EF et BE. Les travaux de (Bouras and Sevasti, 2003) visent une estimation analytique qualitative de la qualité de service offerte par un service de haute priorité. (Trimintzios et al., 2002) proposent une formulation de programmation non linéaire du problème de dimensionnement réseau afin d'utiliser MPLS et DiffServ pour offrir une qualité de service adéquate aux trafics Premium.

2.1.4 EF PHB et Trafic de Voix

La performance de chacune des classes DiffServ est décrite dans plusieurs travaux. Les travaux de (Ferrari and Chimento, 2000) proposent une exploration quantifiée et détaillée des modes d'opération de plusieurs mécanismes de routeur comme l'ordonnancement prioritaire ou WFQ et les méthodes de marquage de paquets impliqués dans l'implémentation du PHB-EF dans les routeurs. La définition du PHB-EF dans (Jacobson et al., 1999) garantit à chaque noeud un taux de transmission supérieur ou égal au débit des flots EF. Ce taux de transmission est garanti quelle que soit la charge de trafic des autres sources moins prioritaire AF ou BE. Le trafic EF occupe la file d'attente la plus prioritaire dans un ordonnancement prioritaire, ou la file de plus grand poids dans un ordonnancement WFQ. Cette définition semble garantir, indépendamment de la taille du réseau, un taux de perte minimal au niveau des noeuds DiffServ, réduisant le temps d'attente en file et la gigue des paquets EF à un strict minimum. Les travaux de (Bennett et al., 2001) montrent un cas de réseau dans lequel la gigue des paquets EF peut être arbitrairement grande à cause de l'accumulation de la gigue, et dépendante de la taille du réseau. Bennett et al. justifient cette contradiction par le fait que la définition citée dans (Jacobson et al., 1999) n'est pas facilement implantable dans les ordonnanceurs connus et qu'elle n'admet pas de tests qualitatifs de conformité. Les auteurs proposent ainsi une définition alternative qui,

à son tour, admet des tests qualitatifs de conformité et proposent des bornes déterministes à la gigue des paquets EF.

Une autre étude sur la gigue des paquets EF est présentée dans (Alshaer and Horlait, 2004). Les auteurs étudient l'effet du trafic d'arrière-plan (background ou BG) sur la gigue des paquets EF. Deux cas sont étudiés. Les paquets EF et BG sont, servis par une file uniservice de type FIFO. Dans ce cas, un paquet EF est servi avant un paquet BG quand les deux arrivent en même temps. En second lieu, les paquets sont servis par deux files, l'une EF prioritaire, l'autre non pour le trafic BG. Alshaer et al. utilisent le simulateur NS-2 pour confirmer leurs résultats analytiques. Les résultats obtenus concordent avec ceux de (Bennett et al., 2001) : la définition du EF PHB dans (Jacobson et al., 1999) est insuffisante pour garantir une gigue minimale aux paquets de la classe EF. La gigue des paquets EF dépend de l'intensité du trafic d'arrière-plan du réseau.

Les travaux de (Vojnović and Leboudec, 2002) permettent d'obtenir une borne probabiliste au délai encouru par les paquets EF. Les modèles présentés sont seulement fonctionnels dans les cas où une courbe de service peut représenter le fonctionnement d'un noeud du réseau et quand chaque flot est uniformisé à l'entrée du réseau. Les auteurs montrent que les bornes obtenues sont exactes pour toute configuration et pour tout nombre de flots.

Plusieurs études, par exemple (Filsfils and Evans, 2002), justifient l'utilisation du PHB-EF pour offrir une qualité de service adéquate au trafic de voix. Les travaux de (Ziviani et al., 1999) comparent les gigues de deux modèles de sources de voix, l'un CBR, l'autre On-Off. Les résultats montrent que la classe EF peut admettre un nombre supérieur de sources On-Off que de source CBR sans changement notable dans la performance du réseau. L'augmentation de la capacité réservée à la classe EF induit une meilleure amélioration de performance pour les sources On-Off. Cette amélioration est bornée par l'ordonnancement prioritaire des files utilisé dans les routeurs DiffServ. Ziviani et al. poursuivent leur étude dans (Ziviani et al., 2002) pour évaluer les délais et les gigues des paquets de

voix quand ils sont classifiés EF.

2.1.5 AF PHB et Trafic Vidéo

Les travaux caractérisant la performance du AF PHB sont multiples. La différenciation de service entre les classes AF est quantifiée par la probabilité de rejet des paquets et leur délai maximum. Un algorithme qui optimise l'allocation des ressources en terme de la taille des tampons et du taux de service est présenté dans (Pham et al., 2004). Les auteurs de (Bensaou et al., 2004) proposent un modèle qui permet de définir des bornes statistiques inférieures et supérieures aux probabilités de rejet associées à deux classes AF dans un réseau DiffServ.

La définition de la classe AF dans (Heinanen et al., 1999) suggère l'utilisation d'une technique de gestion active des files d'attente (tel RED) pour offrir plusieurs niveaux de priorités de rejet. RIO (RED with In/Out) et WRED (Weighted RED) sont deux extensions MRED (Multi Level-RED) possibles. Les résultats montrent que RIO offre une meilleure performance que WRED dans le traitement des paquets moins prioritaires d'un trafic bursty On-Off. Pour les connexions de courte durée, RIO est plus performant. Les deux modèles offrent la même performance pour un trafic de transfert de données.

Les travaux de (Koucheryavy et al., 2003) proposent l'utilisation du AF PHB pour satisfaire les exigences en qualité de service du trafic de vidéo sur demande (VoD). Le trafic VoD peut être classifié comme un des trafics les plus sensibles aux pertes et délais. Le trafic généré par ce type d'application requiert un niveau de qualité de service strict en terme de perte de paquets, délai, et gigue. Les auteurs proposent un service de transmission VoD compatible avec l'implémentation DiffServ. Ces derniers détaillent le fonctionnement d'une source VoD. Des modèles de trafic VoD déterministes et stochastiques sont par la suite explorés. Ces modèles VoD imposent des paramètres de profil de trafic

très spécifiques. Les auteurs décrivent comment adapter le service de transmission du AF PHB à ces paramètres de profil de trafic pour obtenir une garantie de service adéquate.

Toutes ces études visent à optimiser le déploiement de DiffServ dans un réseau IP. Toute la littérature propose d'utiliser DiffServ comme mécanisme de protection contre la congestion. La littérature est riche en travaux qui étudient les effets des différentes configurations des paramètres réseau sur différents types de trafics associés aux classes EF, AF et BE de DiffServ. Des modèles analytiques et statistiques d'une complexité variée ont été proposés pour la quantification exacte de la performance des classes de priorités sous différentes contraintes de trafic et de réseau.

2.2 Mécanismes de protection dans les réseaux IP/WDM

Cette section présente une étude exhaustive des différents mécanismes de protection proposés pour les réseaux IP/WDM.

2.2.1 Mécanisme de protection dans les réseaux WDM

La bibliographie est riche en travaux qui étudient les différents mécanismes de protection disponibles dans les réseaux WDM. Cette section ne relève que les recherches les plus pertinentes au projet doctoral proposé.

La nécessité d'avoir des mécanismes de protection au niveau WDM est justifiée dans (Gerstel and Ramaswami, 2000a). En déployant des réseaux IP/WDM, les opérateurs cherchent à simplifier leurs structures de réseaux. La couche WDM a pour fonction d'assurer des chemins optiques pour les connexions des couches supérieures, notamment la couche IP ou encore la couche client. Les chemins optiques sont donc des conduits établis par commutation de circuits qui opèrent à des grandes vitesses (de 2.5 Gbps à même 10Gbps).

Ces chemins sont généralement établis pour interconnecter des équipements réseau des couches supérieures, par exemple des routeurs IP. Gerstel et al. justifient la nécessité d'incorporer des mécanismes de protection optique au niveau WDM. Ils montrent que les mécanismes des couches supérieures peuvent ne pas être suffisants pour protéger le trafic contre les pannes. Les mécanismes de restauration de la couche IP manquent parfois la rapidité nécessaire pour fournir une QdS adéquate aux différents types de trafic des réseaux IP/WDM. Il importe alors que la couche optique puisse fournir des mécanismes rapides de détection, de restauration et de protection contre les pannes. Les mécanismes de protection et restauration de la couche optique peuvent être considérés comme des mécanismes additionnels utilisables pour augmenter la fiabilité des réseaux. Certains réseaux de transport ne sont conçus que pour offrir une protection en cas de panne simple dans les réseaux. L'occurrence des pannes multiples peut être traitée par les mécanismes de la couche optique inférieure. La couche optique peut être la plus adéquate à traiter certains types de pannes, notamment les coupures de fibre. Au lieu de laisser cours à l'éventuelle propagation de nombreux signaux d'alarme pour traiter les effets de cette panne au niveau des couches supérieures, la couche optique peut directement résoudre ce problème en effectuant un reroutage rapide sur un autre chemin optique avant qu'aucune couche supérieure ne sache qu'il y ait eu une panne.

Gerstel et al. continuent en montrant quelques limitations des mécanismes de protection de la couche optique. La couche optique peut ne pas être en mesure de détecter certains types de problèmes. Les auteurs mentionnent que la couche optique protège le trafic contre les pannes en offrant protection au chemin optique sur lequel il circule. S'il existe une diversité dans la nature du trafic qui parcourt un chemin optique, la couche WDM est incapable de les distinguer. Il faut un mécanisme des couches supérieures pour offrir une protection plus fine pour faire ce genre de protection. Les limitations de budget ou de disponibilité de ressources optiques peuvent poser des contraintes sur la capacité de protection de la couche optique. Ces contraintes se modélisent par exemple, par le nombre de longueurs

d'onde disponibles pour la protection ou le nombre de sauts permis sur un chemin de protection ce qui met en relief l'avantage du modèle de protection DiffServ* qui ne requiert aucune redondance optique.

Les auteurs distinguent entre les différents types de pannes d'équipements optoélectriques. Seuls les plus pertinents à ce projet sont cités. Une panne peut toucher la carte interface entre l'équipement de la couche client et celui de la couche optique. Cette carte, appelée transpondeur, convertit le signal électrique en onde lumineuse suivant une longueur d'onde spécifique au niveau optique. Une carte est nécessaire pour chaque longueur d'onde donc pour chaque chemin optique. Une panne de cette carte engendre une panne de chemin optique. L'autre type de panne considéré est celui des coupures de fibres optiques. Plusieurs longueurs d'onde sont multiplexées à l'intérieur d'une même fibre. La coupure d'une fibre engendre des pertes énormes en bande passante, surtout dans les réseaux WDM. Les auteurs mentionnent que 136 coupures de fibres ont été signalées par les opérateurs américains en 1997.

Gerstel et al. distinguent entre les mécanismes de protection qui fonctionnent au niveau des chemins (ou canaux) optiques d'un réseau (niveau Optical Channel OCh) et les mécanismes de protection qui fonctionnent au niveau Optical Multiplex Section (OMS). Le premier traite les coupures de fibres ainsi que les pannes d'équipements terminaux, par exemple transmetteurs et récepteurs optiques. Ces mécanismes sont recommandés par plusieurs organismes de standardisations tel l'ANSI (American National Standards Institute et l'ITU-T (International Telecommunications Union Telecommunication Standardization Sector). Le second niveau de protection fonctionne au niveau OMS. Ce type de protection ne reconnait pas la différence entre les canaux optiques multiplexés ensemble mais les restaure simultanément en les reroutant par groupe. Les auteurs poursuivent par une description des différents mécanismes de protection WDM des deux niveaux OCh et OMS. Ils décrivent une multitude de mécanismes de protection tel 1 :1, 1+1, 1 :N et de restauration applicable dans les réseaux WDM maillés. Ils survolent aussi les mécanismes

de protection des réseaux en anneau et proposent certains critères pour offrir différents niveaux de protection au niveau des réseaux. Cinq classes sont proposées :

- Services qui doivent être protégés à la couche optique
- Services qui ne doivent pas être protégés au niveau optique
- Services n'exigeant pas de protection optique
- Services à protection Meilleur-Effort.
- Services préemptables qui en temps normal utilisent la bande passante réservée à la protection d'autres services et sont préemptés en cas de pannes.

Gerstel et al. montrent la nécessité de déployer des mécanismes de protection au niveau de la couche WDM mais imposent diverses limitations.

Les travaux de (Ramamurthy and Mukherjee, 1999b) et (Ramamurthy and Mukherjee, 1999a), regroupés dans (Ramamurthy et al., 2003), offrent une vision détaillée des différents mécanismes de protection offerts par la couche WDM. Ces études discutent des différents mécanismes de protection et restauration disponibles dans les réseaux WDM. Ils distinguent deux grandes approches, par chemin optique et la deuxième, par lien optique. Dans le premier cas, si une panne de composante optique affecte un lien d'un chemin optique, la connexion est entièrement redirigée du chemin primaire vers un chemin de protection. Ce dernier peut être préétabli à l'avance (protection) ou calculé dynamiquement suite à la panne (restauration). Dans le cas d'une protection/restauration par lien, les commutateurs optiques directement adjacents à la composante en panne s'occupent de rerouter localement le trafic du lien qui est en panne vers un autre chemin de protection. Nous pouvons voir un exemple de la protection par chemin dans la figure 2.3. Une connexion entre les OXC 1 et 4 est routée sur le chemin optique $[1, 2, 3, 4]$. Suite à une panne du lien $[2, 3]$, la connexion est entièrement reroutée sur le chemin de protection $[1, 5, 6, 4]$. Le deuxième plus court chemin entre l'origine et la destination finale de la connexion est généralement choisi comme chemin de protection. La figure 2.4 montre

une protection locale de la connexion en cas d'une panne du lien $[2, 3]$ où la connexion est reroutée localement et généralement sur le deuxième plus court chemin entre les OXC adjacents à la panne. Nous remarquons que dans le cas d'une protection par lien, la panne est directement détectée par les OXC adjacents et il n'y a aucune nécessité de signaler la panne jusqu'à l'origine de la connexion. Le reroutage est immédiat, mais le chemin de protection le plus court n'est pas toujours garanti.

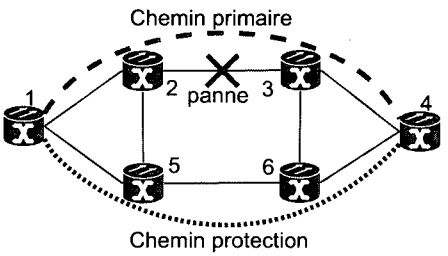


FIG. 2.3 Protection par chemin

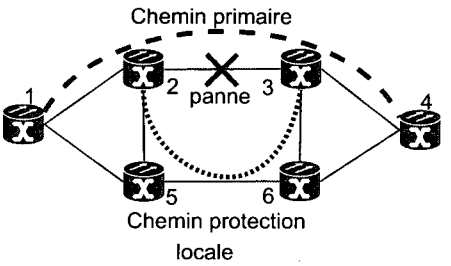


FIG. 2.4 Protection par lien

Les auteurs proposent le diagramme de la figure 2.5 pour montrer les diverses possibilités de protection et restauration dans les réseaux WDM maillés. En ce qui a trait à la protection/restauration par chemin, trois catégories sont définies. Pour une protection par chemin dédié $(1 : 1)$, les ressources du chemin de protection sont réservées à l'usage unique d'une connexion affectée par une panne. Ils ne sont pas partagés avec les ressources d'autres chemins de protection d'autres connexions. La protection par chemin partagé permet le partage des ressources de protection de plusieurs connexions. Les chemins de protection sont entièrement ou partiellement multiplexés sur des chemins optiques identiques. Les chemins optiques protégés ne sont pas censés pouvoir tomber en panne en même temps. Comme un même chemin optique peut être utilisé pour protéger plusieurs connexions à la fois, cette deuxième option permet une meilleure utilisation des ressources du réseau. La restauration par chemin est la dernière option sous cette catégorie. Un chemin de protection est calculé dynamiquement suite à une panne et s'étend de bout en bout, de l'origine jusqu'à la destination. La connexion est entièrement reroutée sur le chemin de protection.

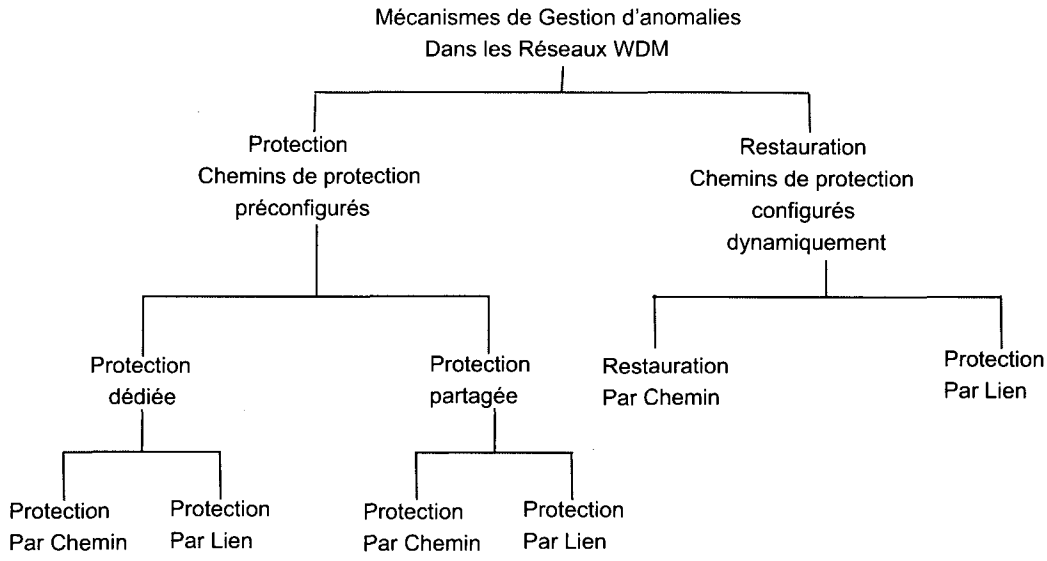


FIG. 2.5 Gestion des anomalies dans un réseau WDM.

Il existe aussi des mécanismes de protection par lien. Le premier consiste en une protection dédiée. Chaque lien du chemin primaire sera muni d'un chemin de protection secondaire. Ce dernier est établi entre le noeud origine et le noeud destination du lien en question. Les ressources des chemins de protection sont entièrement réservées à l'usage des connexions affectées par les pannes. Selon les auteurs de (Ramamurthy et al., 2003), cette option est connue pour être très coûteuse. La figure 2.6 illustre cette inefficacité. La protection du chemin optique $[1, 2, 3]$ nécessite la réservation d'une longueur d'onde sur la fibre $[1, 4]$, deux sur $[4, 2]$ et une quatrième sur $[4, 3]$. Si l'option protection dédiée par chemin est utilisée seule 2 longueurs d'onde sont nécessaires, une sur $[1, 4]$, l'autre sur $[4, 3]$.

En second lieu, le problème de protection dédiée par lien peut être résolu en utilisant l'option de protection partagée par lien. Les longueurs d'onde réservées en guise de protection peuvent être partagées parmi plusieurs connexions. On suppose dans ce cas que deux connexions qui partagent les mêmes ressources de protection ne s'attendent pas à subir des pannes simultanées de leurs chemins optiques respectifs. Dans ce cas, trois longueurs d'onde seront nécessaires pour la protection du chemin $[1, 2, 3]$, deux dédiées sur $[1, 4]$

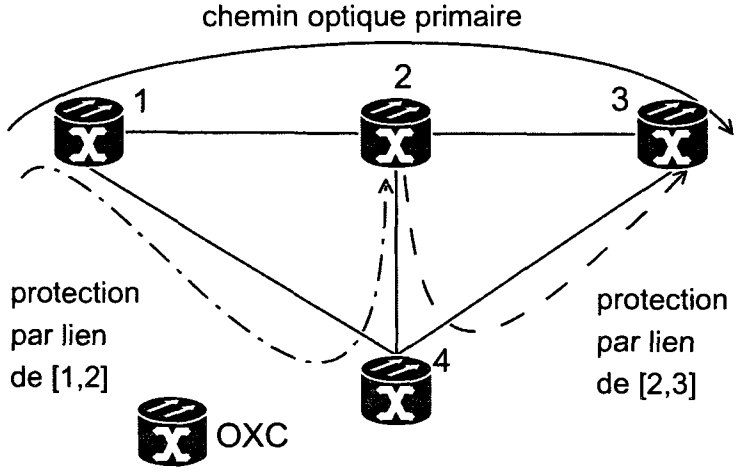


FIG. 2.6 Protection dédiée par lien, exemple d'inefficacité.

et $[4, 3]$, une partagée sur $[4, 2]$ (nous supposons une réservation bidirectionnelle des ressources). Enfin, la dernière option est celle d'une restauration par lien. Les OXC adjacents à la fibre en panne s'occupent de rétablir leurs connexions perdues en trouvant dynamiquement un chemin secondaire. Si aucun chemin n'est trouvé, les connexions traversant la composante en panne seront coupées.

Ramamurthy et al. proposent et comparent les trois modélisations mathématiques en nombres entiers suivantes. La première a pour objectif de minimiser la capacité totale utilisée en optant pour la protection dédiée par chemin ; la deuxième minimise la capacité totale utilisée dans le réseau avec protection par chemin ; la dernière considère la protection par lien partagé tout en gardant le même objectif de minimiser la capacité totale utilisée dans le réseau. Les auteurs montrent dans (Ramamurthy et al., 2003) qu'une solution peut être atteinte pour des réseaux de petite taille et quelques dizaines de noeuds. Des méthodes heuristiques sont cependant nécessaires pour des réseaux de grandes tailles de quelques centaines de noeuds. Les résultats montrent principalement que la protection par chemin partagée est plus avantageuse par rapport aux 2 autres. Ainsi l'option de protection partagée par chemin peut être retenue dans le cas du trafic de moyenne priorité.

Les auteurs citent aussi un grand nombre de références qui traitent de la conception de réseaux WDM fiables. Parmi ces dernières, nous trouvons (Bonenfant, 1998) et (Gerstel and Ramaswami, 2000a) qui traitent les notions de capacité de survie des réseaux WDM. (Zhou and Subramaniam, 2000) et (Gerstel and Ramaswami, 2000b) analysent la protection 1+1, mais aussi d'autres types de protections optiques applicables aux architectures de réseaux WDM. (Zhou and Subramaniam, 2000) donnent une grande importance à la résistance aux pannes d'un réseau WDM. Cette résistance est d'autant plus importante quand une panne de fibre engendre des pertes de bande passante dans l'ordre des gigabits et térabits par seconde. Les travaux de (Medard et al., 1999) proposent un algorithme de protection contre les pannes de noeuds et liens dans les réseaux optiques. Leur algorithme utilise le concept de création d'arbres de redondance sur des réseaux WDM. L'algorithme s'assure que chaque noeud est connecté à la racine des arbres par au moins un arbre de redondance et propose un mécanisme de restauration rapide et flexible adaptable à différentes topologies de réseaux optiques. Diverses méthodes analytiques ont été proposées dans (Limal et al., 1998) pour estimer la capacité maximale requise pour assurer un réseau WDM fiable contre les pannes simples de liens.

Une analyse des différents mécanismes de gestion d'anomalies dans les réseaux WDM est présentée dans (Zhang and Mukherjee, 2004). Les auteurs révisent les concepts de base et défis liés à la conception d'un réseau WDM fiable. Plusieurs mécanismes de protection et restauration sont discutés. Zhang et al. citent divers paramètres qui peuvent être utilisés pour mesurer la qualité de service offerte aux protocoles des niveaux supérieurs (IP, ATM, etc.) par la couche d'un réseau WDM maillé. Parmi ces paramètres, la probabilité de disponibilité de service en cas de panne, le degré de fiabilité du service, le temps de restauration et le coefficient de rétablissement de service.

Une liste des principaux mécanismes de protection proposés pour la couche WDM est présentée dans (Maier et al., 2002). Les mécanismes les plus communément adoptés dans les réseaux en anneaux ou maillés sont expliqués. Les auteurs cherchent à utiliser

les fonctionnalités de la couche WDM pour offrir une protection rapide qui assure un rétablissement de service en moins de 50 ms comparativement aux 60 et 100 ms des réseaux SONET et SDH.

2.2.2 Mécanismes de protection et restauration du niveau IP

Une panne de composante, routeur ou lien IP, cause intrinsèquement un changement topologique qui peut être très important en cas de pannes multiples. Les mécanismes de routage dynamique de la couche IP ont la caractéristique de pouvoir s'adapter à ce changement topologique. Une panne est détectée par ses éléments réseau adjacents, l'information est propagée au restant des noeuds fonctionnels, les tables de routages sont mises à jour dynamiquement et les flots IP seront reroutés en conséquence. Couplant ces mécanismes avec un protocole de transport fiable, par exemple TCP, la couche IP est naturellement dotée de mécanismes relativement capables d'offrir un certain niveau de protection/restauration contre les pannes. Selon (Metz, 2000), la dimension temporelle associée aux mécanismes de routage IP limite son utilité vis-à-vis des exigences en QdS des applications temps réel. Plusieurs dizaines de secondes sont habituellement nécessaires à la couche IP pour détecter la panne, signaler cette occurrence aux autres routeurs et recalculer toutes les routes. La majorité des applications temps réel ne peuvent tolérer plus de quelques dizaines ou au plus quelques centaines de millisecondes d'indisponibilité de service. Certaines applications pourront souffrir plusieurs minutes en indisponibilité de service, avec seulement quelques-unes de ces pannes IP. Ceci ralentit grandement la progression vers un réseau IP/WDM compétitif donc disponible pendant au moins 99.999% du temps.

Le routage dynamique de la couche IP est difficilement contrôlable car les routeurs calculent de façon permanente les routes choisies en fonction des dernières informations topologiques du réseau reçues. Dans un réseau IP, les flots sont généralement routés sur les chemins les plus courts. Ceci est connu pour créer une disproportion dans la distribution

de la charge de trafic sur la totalité du réseau. Les flots sont routés sur leurs chemins les plus courts même s'ils sont congestionnés, alors que des chemins légèrement plus longs et plus efficaces en terme de QdS restent inutilisés.

Multiprotocol Label Switching (Rosen et al., 2001) ou MPLS a été créé pour accélérer le processus d'acheminement des paquets IP à destination et de permettre de faire de l'ingénierie de trafic (TE) dans les réseaux IP. MPLS permet la création explicite de tunnels de communication le long d'un chemin composé de routeurs IP munis de capacités MPLS (Label Switching Router ou LSR). Le tunnel créé pour une communication est appelé un Label Switched Path (LSP). L'information portant l'étiquette (Label) d'un LSP particulier est routée explicitement sur le même chemin de ce dernier. L'application la plus intéressante de MPLS sera le TE qui vise à optimiser l'utilisation des ressources d'un réseau en dirigeant les flots IP sur des tunnels créés suivant des critères autres que le coût minimum ou le nombre de sauts minimums. Le chemin le moins congestionné peut être explicitement choisi pour offrir la meilleure QdS possible aux applications temps réel.

MPLS permet aussi de protéger le trafic IP contre les pannes. Un LSP primaire peut être muni d'un LSP de protection. Ce dernier peut être établi à l'avance comme la protection 1 : 1 de la couche optique ou établi dynamiquement suite à une panne pour une restauration :

- locale pour contourner uniquement l'élément en panne ;
- globale donc de bout en bout entre le premier et dernier LSR d'un LSP affecté par la panne.

La restauration du service est rapide, dans moins de 50 ms, seulement dans le cas d'une protection locale où le tunnel de protection à déjà été calculé à l'avance. Dans le cas d'une protection par chemin globale, la protection MPLS nécessite un protocole de signalisation pour propager l'information sur la panne au premier LSR du LSP en panne pour qu'il reroute le trafic sur le LSP de protection. Si ce dernier n'est pas préétabli, il faudra, en plus de la signalisation, activer le protocole Label Distribution Protocol (ou LDP) pour créer

et mettre en place un nouveau LSP de secours. Cette opération peut nécessiter plusieurs secondes avant que le service soit rétabli (Metz, 2000).

Une extension de MPLS, Generalized-MPLS, ou GMPLS (Mannie and Papadimitriou, 2004) permet de contrôler le routage des flots non seulement au niveau IP, mais aussi aux niveaux TDM, longueur d'onde et fibre. Un exemple de la différenciation de service dans les réseaux GMPLS est proposé dans (Kim et al., 2003). Les auteurs proposent des modèles de protection hiérarchique qui optimisent l'utilisation des ressources du réseau en question. Ces derniers proposent trois hiérarchies de LSP optiques : les lambda-LSP (L-LSP), les WaveBand-LSP (WB-LSP) et les fibre-LSP (F-LSP). Chaque type de LSP est muni d'un niveau de protection qui lui est propre, protection $1 + 1$ pour les F-LSP, $1 : 1$ pour les WB-LSP et $1 : n$ pour les L-LSP. La hiérarchie de LSP peut être allouée aux classes EF, AF et DF (Default Forwarding) pour offrir de la différenciation de service.

Les fournisseurs de services Internet prédisent une augmentation annuelle entre 50% et 300% du trafic Internet annuel. Les demandes agrégées en bande passante vont bientôt dépasser les centaines de térabits pas seconde (Fumagalli and Valcarenghi, 2000). Les applications Internet deviennent non seulement exigeantes en bandes passantes, mais aussi en fiabilité. Les auteurs examinent et comparent les avantages et inconvénients des différents mécanismes de protection et restauration disponibles au niveau WDM qu'au niveau IP. Déjà, les résultats montrent qu'il sera nécessaire de combiner l'utilisation des mécanismes de protection et restaurations des deux couches. Les auteurs proposent ensuite une approche heuristique qui permettra d'optimiser l'utilisation conjointe des mécanismes de fiabilités des deux couches. Fumagalli et al. citent la nécessité d'avoir une coordination entre les différents mécanismes pour éviter le déclenchement concurrent de divers mécanismes dans diverses couches pour remédier à la même panne. La coordination est atteinte utilisant des stratégies progressives de signalisation et d'activations de mécanismes en fiabilité. Ces stratégies peuvent être de bas en haut ou de haut en bas.

Selon (Sahasrabuddhe et al., 2002), la forme prédominante de pannes dans les réseaux optiques est la panne simple de fibre. Ceci est comparé aux évènements de pannes multiples dans lesquels plusieurs fibres optiques sont sectionnées simultanément à différents endroits du réseau. Pour faire face à ce type de pannes simples, deux options sont possibles. Au niveau optique, les auteurs considèrent l'établissement d'un chemin optique de protection pour chaque chemin optique primaire. L'autre sera d'utiliser les mécanismes de restaurations de la couche IP pour dévier le trafic autour des éléments en panne ce qui requiert un surdimensionnement de la capacité logique des liens IP pour contenir le trafic supplémentaire en cas de panne. Les auteurs considèrent un réseau IP/WDM et une matrice de trafic donnée et ils cherchent une topologie virtuelle et une assignation de flot qui fournira une protection contre l'évènement d'une panne simple qui maximise la fraction maximale de trafic protégé contre une coupure de fibre.

Dans tout ce qui précède, une panne de fibre ou de chemin optique au niveau WDM implique directement une panne d'un ou plusieurs liens logiques au niveau IP. Si aucune protection n'est offerte au niveau optique, tout le trafic routé sur le(s) lien(s) IP en panne est affecté. Une route alternative doit être calculée pour chaque flot.

Pour réduire le coût associé aux mécanismes de protection optiques, divers auteurs proposent de combiner l'utilisation de ces dernières avec celles des couches IP et MPLS. Plusieurs mécanismes de protection et restauration multicouche ont été proposés, mais tous requièrent une synchronisation et une coordination entre les diverses couches. Ceci induit une complexité accrue pour assurer une fiabilité adéquate dans les réseaux IP/WDM.

Finalement, un livre de référence (Vasseur et al., 2004) explique les avantages, désavantages et défis de déploiement des principaux mécanismes de fiabilité disponibles à différents niveaux des réseaux IP, MPLS, Sonet et optiques contemporains.

2.2.3 Routage IP/WDM de survie

La couche IP connaît seulement le reroutage de flot comme mécanisme pour remédier aux pannes de liens IP. Ce mécanisme est lent, parfois complexe et donc doit être utilisé seulement comme dernier recours. Il serait alors convenable de prévoir une technique qui permet de réduire cette occurrence.

La notion de routage de connexion optique de survie n'est pas étrangère à la littérature. Cette dernière à pour but de garantir la connexité d'une topologie IP suite à une panne d'une composante physique, généralement une fibre optique. Étant un problème NP-complet (Modiano and Narula-Tam, 2002), il existe plusieurs approches plus simples au problème de routage optique de survie.

Selon (Kurant and Thiran, 2005) chaque lien logique de la couche IP est une demande de connexion optique et cette dernière doit être routée sur un chemin optique de la couche WDM. Habituellement, une même fibre peut regrouper plusieurs chemins optiques. Ainsi, une panne simple d'une fibre engendre la panne simultanée de plusieurs liens logiques du niveau IP. Ces pannes de liens IP sont détectées par les routeurs IP et une restructuration du routage des flots IP est déclenchée. Les flots affectés par des pannes de liens sont reroutés sur des chemins de remplacement. La topologie IP doit rester suffisamment connexe après la panne pour garantir la disponibilité des chemins secondaires recherchés. Un exemple pour illustrer ce phénomène est présenté à la figure 2.7. La partie gauche de la figure montre un routage optique intelligent des liens logiques sur les chemins optiques disponibles. La demande de connexion du lien IP (A, B) est routée sur le chemin optique $[1, 4, 2]$. Le lien IP (A, C) est routé sur le chemin optique $[1, 3]$. Le lien IP (C, B) est routé sur le chemin optique $[3, 2]$. Si la fibre $[1, 4]$ est coupée, seul lien IP (A, B) est en panne et le trafic qui circulait sur (A, B) est rerouté sur le chemin (A, C, B). La partie droite de la figure 2.7 montre que (A, B) est mis en place sur $[1, 4, 2]$, (A, C) sur $[1, 4, 3]$ et (C, B) sur $[3, 4, 2]$. Cette option réduit le coût du réseau optique en éliminant le besoin des fibres

$[1, 3]$ et $[3, 2]$. Une coupure de la fibre $[1, 4]$ résultera en une panne des liens IP (A, B) et (A, C). Le réseau IP n'est plus connexe, le noeud A est complètement isolé du réseau et tout trafic de et vers A doit être rejeté.

Les auteurs proposent dans (Kurant and Thiran, 2005) un nouveau concept de "piecewise survivability" en divisant la topologie IP en plusieurs sous-réseaux. Cette approche permet d'un côté de prouver l'existence d'un routage de survie pour une topologie de réseau donnée. Et d'un autre côté, l'algorithme permettra de retracer et de renforcer les endroits les plus fragiles d'un réseau IP/WDM. Les auteurs terminent en proposant un algorithme qui fait du routage de survie de façon efficace et qui permet le passage à l'échelle.

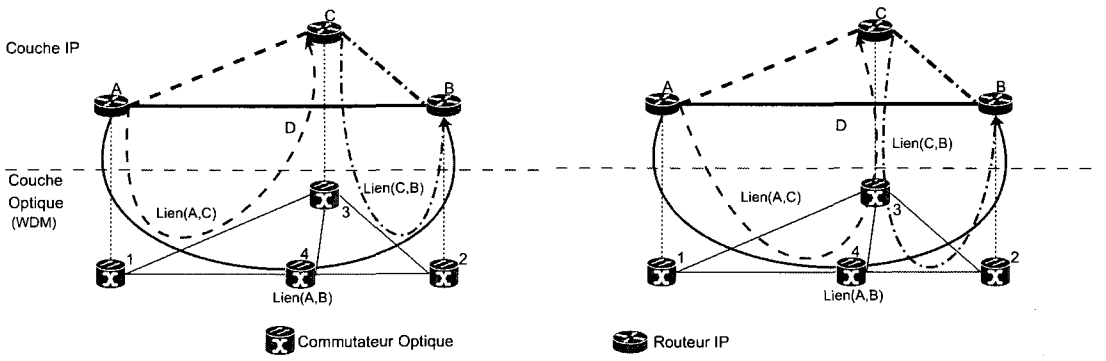


FIG. 2.7 Routage de survie des connexions optiques

OSPF-ECMP (Equal Cost Multipath) est une variante connue de OSFP qui exploite la présence de plusieurs chemins à coûts égaux entre une source et une destination. Pour éviter d'encombrer un chemin avec la totalité du trafic, ce dernier est divisé entre les chemins à coûts égaux et est transmis par la suite à destination.

Une extension à OSFP est proposée dans (Schneider and Nemeth, 2002). Se basant sur le concept de OSPF-ECMP (Equal Cost Multipath). Les auteurs étudient la performance de OSFP-OMP (Optimized Multiplath). L'algorithme essaie de trouver dynamiquement l'allocation optimale de trafic aux divers chemins à coûts égaux trouvés. Les auteurs développent un simulateur à évènements discrets pour caractériser leur approche.

Selon (Crochat and LeBoudec, 1998), la protection dans les réseaux WDM peut être réalisée à deux niveaux, l'un physique et l'autre au niveau de la conception. La protection physique du niveau WDM fournit une base de transport fiable aux niveaux supérieurs. Cette option est coûteuse parce qu'elle propose une duplication de l'infrastructure physique, mais reste très simple à gérer. Le concept de protection par conception (Design Protection) maintient la connectivité entre toutes les paires de ports réseau, mais ne garantit pas que la totalité du trafic sera protégée suite à une panne de composante optique. La couche supérieure du réseau (IP dans le cas d'un réseau IP/WDM) doit se reconfigurer de façon à ce que seuls les trafics de hautes priorités soient transportés en cas de pannes.

Les auteurs de (Crochat et al., 2000) proposent l'algorithme PIW (Protection Interoperability for WDM) pour apporter une solution aux problèmes engendrés par le phénomène de propagation d'une panne du niveau optique au niveau supérieur d'un réseau. En considérant un réseau IP/WDM, deux routeurs adjacents du niveau IP sont vus comme étant reliés par un lien logique direct. Ce lien logique est établi au niveau optique par une concaténation de liens physiques. Cette concaténation est usuellement connue sous le nom de chemin ou canal optique. Dans le cas d'une panne d'un lien physique, un ou plusieurs liens du niveau supérieur peuvent, par phénomène de propagation, être affectés. La connectivité du réseau logique peut être grandement affectée puisque la couche logique tentera de restaurer cette connectivité par reroutage des flots sur des liens fonctionnels. Ce reroutage peut engendrer des problèmes de congestion majeurs. Une possibilité sera de rendre invisibles les pannes du niveau optique au niveau supérieur et cette option requiert l'utilisation des mécanismes de protection et restauration connus de la couche WDM. Une autre possibilité sera d'assurer un routage intelligent des connexions logiques sur les chemins optiques. Les auteurs suggèrent ainsi un algorithme qui limite la propagation de pannes et s'assure que le réseau logique reste suffisamment connexe suite à une panne et garde suffisamment de ressources pour effectuer les opérations de reroutage des flots sans causer de congestion majeure.

Les auteurs de (Veerasamy et al., 1994) explorent la notion de division de trafic sur plusieurs chemins, mais seulement suite à une panne. Quand une panne affecte le chemin principal d'un flot, le trafic de ce flot est subséquemment divisé sur un ou plusieurs chemins de protection. Une division égale a lieu quand la moitié du trafic est reroutée sur un chemin de protection, l'autre partie sur un autre chemin. Une autre option serait de rechercher tous les chemins de protections possibles et envoyer une petite partie du flot affecté sur chaque chemin de protection. Les auteurs, évaluant la performance de chaque option, concluent que la seconde méthode s'avère plus complexe que la première, mais résulte en une économie majeure en termes de surdimensionnement de la bande passante du réseau.

2.3 Protection différenciée dans les réseaux

La tendance courante dans le développement des réseaux est d'offrir une solution unifiée qui offre support à différents types de trafic de voix, de données et de multiples services multimédias. Dans le but de garantir une capacité de survie différenciée aux diverses priorités de trafics, il devient primordial d'unifier la différenciation de service avec la tolérance aux pannes dans les réseaux IP-Optique.

2.3.1 Probabilités de protection et protection différenciée

Une approche à la protection différenciée est présentée dans (Xiang et al., 2004). Les auteurs décrivent un réseau WDM comme étant un ensemble de commutateurs WDM reliés par des liens de fibres optiques. Les auteurs citent plusieurs références, dont (Ramamurthy and Mukherjee, 1999b; Ramamurthy and Mukherjee, 1999a) qui ne spécifient que deux nivaux de fiabilité par connexion optique, 100% protégée ou non protégée. Les auteurs citent aussi (Saradhi and Murthy, 2002) pour justifier leurs travaux. Ils mentionnent que les pannes des composantes de réseau sont aléatoires surtout pour des réseaux de grande

taille. Dans cet environnement aléatoire, un fournisseur de service ne peut offrir à son tour que des garanties statistiques en cas de pannes. On appellera probabilité de protection, la probabilité avec laquelle une protection est garantie pour une connexion. Il est aussi possible d'associer les différents niveaux de fiabilité requis par les différents services à des probabilités de protection. Xiang et al. proposent alors un algorithme, le QdS-Based Partial Protection algorithm based on wavelength layered graph (QPP-LG), qui optimise l'utilisation des ressources du réseau WDM en offrant une option de protection partielle aux différentes connexions du réseau. L'algorithme est inspiré du problème de Routing and Wavelength Assignement (RWA) pour attribuer les longueurs d'onde du niveau optique aux connexions de la couche supérieure. Chaque demande de connexion est routée de façon prioritaire au niveau optique. Si le chemin choisi est incapable d'offrir le niveau de fiabilité adéquat, un chemin de protection partielle ou de bout-en-bout doit être établi pour cette connexion. L'algorithme essaie de trouver un chemin de protection partiel adéquat qui correspond à la probabilité de protection requise par la connexion. Si ce dernier n'est pas trouvé, le chemin de protection de bout-en-bout est considéré.

Les auteurs de (Saradhi and Murthy, 2004) proposent à leur tour un algorithme pour l'établissement dynamique de canaux optiques à degrés de survies différenciés dans les réseaux WDM. La qualité de service fournie à un flot est définie par le type de chemin optique primaire et de protection utilisés. Le nombre de chemins de protections par chemin primaire définira le niveau de fiabilité offert à une connexion par la couche WDM. Les auteurs distinguent sept classes :

- un chemin primaire dédié et un chemin de protection dédié ;
- un chemin primaire dédié et plusieurs chemins de protection dédiés ;
- un chemin primaire dédié et un chemin de protection partagé ;
- un chemin primaire partagé et un chemin de protection partagé ;
- un chemin primaire partagé et plusieurs chemins de protection partagés ;
- un chemin primaire dédié multisauts et un chemin de protection dédié multisauts ;

– un chemin primaire partagé multisauts et un chemin de protection partagé multisauts.

Les auteurs procèdent par simulation pour montrer l'efficacité de leur méthode en terme de tolérance aux fautes, aux délais, aux bandes passantes et aux disponibilités des ressources.

2.3.2 Disponibilité des ressources et protection différenciée

Les auteurs de (Zhang and Durresi, 2002) explorent la nécessité, les méthodes et les avantages de la coordination des mécanismes de survie entre les différentes couches dans les réseaux IP/WDM. Zhang et al. citent les différents facteurs impliqués dans la conception d'un réseau IP/WDM fiable : l'utilisation efficace des ressources, le taux de blocage d'appel, le temps de restauration, le taux de rétablissement, la complexité, la granularité, la tolérance aux pannes simples ou multiples et l'extensibilité. Les auteurs proposent un compromis entre la capacité de survie et l'utilisation des ressources du réseau. Ils considèrent que, quand les ressources du réseau sont rares, à cause d'une panne de fibre par exemple, le taux de survie des trafics de basses priorités peut être relaxé pour accommoder plus de trafic de haute priorité. Ils justifient leur raisonnement par le fait que les coupures de fibres sont assez rares dans les réseaux IP/WDM.

Suite à une description et une comparaison qualitative des différents mécanismes de protection et restauration dans les réseaux maillés IP/WDM, Zhang et al. proposent trois niveaux de résilience à trois classes prioritaires de trafic. Bien qu'il soit souhaitable de fournir un niveau de résilience à 100% garanti à tous les types de trafic du réseau, cette solution est à la fois irréaliste, inefficace et parfois inutile pour du trafic courriel par exemple.

Ainsi, les auteurs proposent de fournir une protection garantie à 100% aux trafics à haut niveau de résilience, quand les ressources du réseau le permettent, une protection 1+1 ou 1 :1 est suggéré pour ce cas. Une protection partagée 1 : N est suggérée pour le trafic à niveau de résilience moyen. Finalement, aucune protection immédiate n'est prévue pour

le trafic à bas niveau de résilience. Ceci s'explique par le fait que ce dernier type de trafic est capable de tolérer les interruptions de service. Ils suggèrent par contre de prévoir des mécanismes de restauration dynamiques en cas de pannes.

Les auteurs complètent leur article en proposant pour les couches IP/GMPLS et WDM, un modèle de protection adéquat qui est exprimé à la fois en fonction du type de trafic et de la disponibilité des ressources. Ils terminent leur étude en suggérant un modèle de coordination des mécanismes de survie des deux couches. Cette coordination doit être minutieusement établie pour éviter les effets indésirables de l'activation parallèle des mécanismes de protection des deux couches suite à une même panne dans le réseau.

2.3.3 Protection différenciée par modélisation par arborescence

Une architecture multicouche de services de protection différenciée est proposée dans (Naser and Mouftah, 2004). Les auteurs modélisent leurs réseaux en utilisant une architecture à huit couches. Plusieurs flots de paquets IP sont multiplexés dans un lien MPLS (Label Switching Path ou LSP). Un ou plusieurs LSP passent dans un lien TDM de plus grande capacité. Un ou plusieurs liens TDM sont multiplexés dans une longueur d'onde. Plusieurs longueurs d'onde sont regroupées dans un lien appelé gamme de longueurs d'onde. Plusieurs gammes forment une fibre. Plusieurs fibres forment un câble. Plusieurs câbles traversent un conduit, plusieurs conduits passent par, ce que les auteurs appellent, un Right of Way (RoW). Les couches fibre, câble, conduit et RoW forment les ressources physiques du réseau. Les couches supérieures constituent les ressources logiques.

Plusieurs propriétés émergent d'une telle architecture. Naser et al. citent par exemple, l'héritage de panne. Quand un lien d'une couche quelconque tombe en panne, tous les liens des couches supérieures traversant le lien en panne en sont affectés. Cet héritage peut être multiple. Un lien IP peut être constitué d'une concaténation de LSP et si un

LSP tombe en panne, le lien IP partage le même sort. Finalement, le concept d'héritage de bande passante est défini. Si une capacité C est réservée pour une connexion à un niveau supérieur, cette même capacité doit être réservée au niveau des toutes les couches inférieures. L'héritage de panne se fait de bas en haut, l'héritage de bande passante se fait de haut en bas. Les auteurs proposent une arborescence (Shared Risk Link Group (SRLG)) pour modéliser cette architecture mutlicouche. La racine de l'arbre peut représenter par exemple un lien IP, les descendances immédiates de cette racine sont par exemple des LSP. Les descendances des LSP sont des liens TDM, etc. Les auteurs utilisent leur SRLG pour proposer un mécanisme capable de fournir plusieurs classes de protection différenciée dans un réseau multicouche.

2.3.4 Qualité de service différenciée dans les réseaux WDM

Une mise au point sur l'importance de la fiabilité des réseaux et les différentes méthodes capables de fournir une différenciation de service dans les réseaux WDM survivable est réalisée dans (Saradhi et al., 2004). Ces méthodes sont classifiées selon différents critères comme la fiabilité différenciée (Differentiated Reliability), les connexions-R (R-Connexions), la qualité de protection (Quality of Protection), et la qualité de rétablissement (Quality of Recovery). Une grande tendance actuelle est de développer un réseau qui unifiera une multitude de services, la voix, la vidéo, les données et d'autres trafics multimédias variés. Différentes applications exigent différents niveaux de tolérances aux fautes, temps de rétablissement et le prix pour obtenir le niveau de service adéquat. Les auteurs établissent une dépendance proportionnelle entre la fiabilité d'une protection et le coût associé à cette fiabilité. Plus une connexion est fiable plus son coût d'établissement sera grand. Il existe plusieurs options de protection dans les réseaux optiques, connues sous le nom de classes de fiabilité de service (Reliability of Service (RoS)) et les auteurs en distinguent 4 :

– connexions à protection garantie : un canal optique de protection dédié par canal pri-

maire ;

- connexions à protection meilleur effort : un canal optique de protection est disponible seulement si les ressources sont disponibles ;
- connexions non protégées : aucune protection n'est offerte à ces connexions ;
- connexions préemptables : ces connexions sont délibérément coupées suite à une panne pour libérer les ressources et assurer la protection d'autres connexions plus prioritaires.

2.3.5 Fiabilité différenciée

La première méthode étudiée par les auteurs de (Saradhi et al., 2004) est celui des connexions à fiabilité différenciée (Differentiated reliable connections DiR). Les auteurs font preuve d'un intérêt considérable envers le concept qui consiste à fournir des classes de fiabilité variée pour inclure toutes les classes de services sur un spectre continu de niveaux de protection. Utilisant DiR, chaque connexion apartient à une classe c et possède une probabilité $P(c)$ maximale de panne (Maximum Failure Probability (MFP)). Cette valeur indique que dans le cas d'une panne simple, la connexion est maintenue avec une probabilité $1 - P(c)$. Les auteurs citent (Fumagalli and Tacca, 2001) pour montrer l'application du concept de DiR dans la conception des réseaux optiques en anneau et (Fumagalli et al., 2002) pour montrer l'extension et l'application du concept DiR aux réseaux WDM maillés avec protection partagée.

Le deuxième concept proposé par les auteurs de (Saradhi et al., 2004) est celui des connexions-R (Reliable connections ou R-connections). Les auteurs citent (Saradhi and Murthy, 2002) pour exposer ce concept. Une connexion avec une exigence de fiabilité est appelée une connexion-R. Dans ce contexte, la fiabilité d'une ressource ou d'une composante réseau est définie comme étant la probabilité que cette composante fonctionne pendant un intervalle de temps donné. Si r_i représente le niveau de fiabilité requis par le lien i, $\prod_{i=1}^{n} r_i$ est définie comme la fiabilité du chemin composé des liens $i = 1...n$ et

en supposant l'indépendance des évènements de panne. L'algorithme présenté dans (Saradhi and Murthy, 2002) établit pour chaque connexion un chemin optique primaire et un chemin de protection optionnel. Le chemin de protection n'est envisagé qu'au cas où le chemin primaire n'offrirait pas le niveau de fiabilité voulu. Ce dernier est augmenté quand le chemin primaire est muni d'un chemin de protection. Le chemin de protection peut être de bout-en-bout ou partiel selon des besoins de la connexion. Un algorithme similaire est présenté dans (Xiang et al., 2004). Les auteurs de (Saradhi and Murthy, 2002) calculent la fiabilité d'un chemin primaire muni d'un chemin de protection partielle ou totale, comme étant égale au produit du degré de fiabilité de la portion du chemin primaire non couverte par le chemin de protection par le degré de fiabilité du segment primaire et du segment de protection ensembles. Si nous prenons l'exemple de la figure 2.8, soit r_p la fiabilité du segment du chemin primaire, r_s la fiabilité du segment primaire protégé $[A2 - A3 - A4 - A5]$ et r_b la fiabilité du segment de protection partielle $[A1 - B7 - B8 - B9 - A5]$. La fiabilité totale du chemin principal muni de son chemin de protection partielle est de $r_c = (r_p/r_s)(r_s + r_b(1 - r_s))$. Si le chemin de protection n'existe pas $r_b = 0$ donc $r_c = r_p$. Si le chemin de protection est de bout-en-bout (protection totale) alors $r_s = r_p$ et $r_c = r_s + r_b(1 - r_s)$.

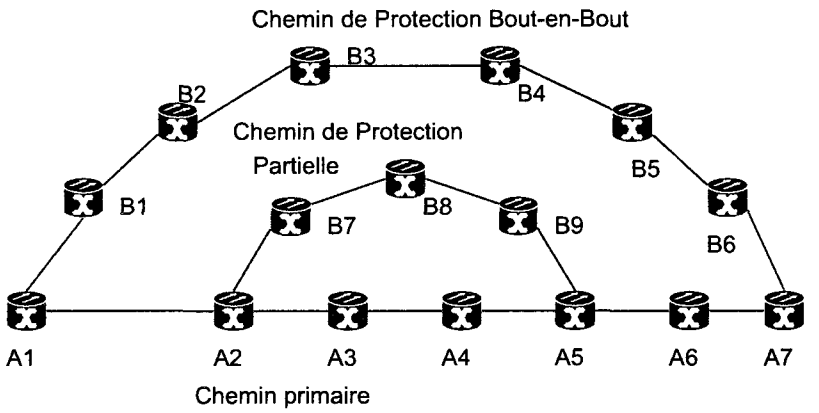


FIG. 2.8 Protection Partielle Différenciée

2.3.6 Qualité de protection

Les auteurs de (Saradhi et al., 2004) continuent leur revue de littérature en passant à la notion de Qualité de protection. Les auteurs résument les travaux de (Gerstel and Sasaki, 2001) pour décrire la conception des topologies logiques utilisant la notion de qualité de protection.

D'après (Gerstel and Sasaki, 2001), les réseaux SONET/SDH en anneaux actuels utilisent au moins 50% de leur bande passante en guise de protection garantie. Ce gaspillage de bande passante devient de plus en plus inacceptable et représente une motivation importante pour délaisser la protection en anneau simple pour la protection en grille plus complexe, mais plus efficace. Les auteurs dans (Gerstel and Sasaki, 2001) proposent une approche quantifiée à la notion de qualité de protection (QoP). Quatre classes de protection sont discutées. La première offre une protection garantie typiquement à 99.999%. La deuxième classe offre une protection probabiliste meilleur effort aux connexions optiques. Soit $B(C)$ la bande passante requise par une connexion de cette classe. La QoP offerte à cette connexion est déterminée par la probabilité $Q(C)$ avec laquelle le service sera immédiatement rétabli suite à une panne. Une valeur de $Q(C) = 1$ indique que la connexion sera entièrement rétablie (protection garantie) suite à une panne alors qu'une valeur de $Q(C) = 0$ indique qu'aucune protection n'est offerte à la connexion en cas de panne. La classe Meilleur Effort spécifie une valeur variable $0 < Q(C) < 1$ pour ces connexions. Les différentes valeurs de $Q(C)$ correspondent à différents niveaux de service offerts par cette classe. La troisième classe proposée par les auteurs est celle des connexions non protégées où $Q(C) = 0$. La quatrième classe de service offerte est celle des connexions préemptables. Les liens réservés en guise de protection peuvent être utilisés par du trafic préemptable. Ce trafic est immédiatement préempté par le trafic protégé avec l'occurrence d'une panne. Différents niveaux de préemption sont proposés pour déterminer la priorité de préemption des connexions qui utilisent le lien de protection. Cette priorité est définie

par une valeur $-1 < Q(C) < 0$. Les auteurs proposent ainsi un paradigme unifié qui place toutes les classes mentionnées ci-dessus sur un spectre continu de niveaux de protection. À chaque connexion est assignée une QoP garantie. La probabilité qu'une connexion soit rétablie suite á une panne est déterminée par sa QoP.

Les auteurs de (Gerstel and Sasaki, 2001) soulèvent un point important à l'effet que la majorité des pannes se produisent au niveau IP et ne peuvent pas être réparés par des mécanismes de la couche optique. Nous pouvons alors nous demander pourquoi offrir des garanties de 99.999% de protection quand les autres éléments réseaux sont très loin de ce niveau de fiabilité.

Les auteurs de (Ming et al., 2005) proposent deux algorithmes de routages, le MDQR (minimum delay QoP routing) et le MAQR (maximum aggregation QoP routing) pour assurer une allocation efficace des ressources réseaux parmi les connexions différenciées par leurs niveaux de QoP. Ils montrent l'efficacité de leurs algorithmes en terme de performance de blocage et capacité à fournir des services à capacités de survie différenciées.

2.3.7 Qualité de fiabilité

Pour décrire la conception des topologies logiques utilisant la notion de qualité de fiabilité (Quality of reliability (QoR)), les auteurs résument les travaux de (Arakawa et al., 2003). Cet article définit la qualité de fiabilité comme étant la réalisation de la QdS en respectant la fiabilité requise au niveau WDM des réseaux. Dans cet article, la QoR est définie par le temps de rétablissement de service suite à une panne, soit l'intervalle de temps entre le début de la panne et le moment de reroutage du trafic du chemin primaire en panne sur le chemin de protection. Les différentes classes de QoR sont identifiées par QoR_1 pour indiquer la classe de plus haute priorité. Le trafic de cette classe aura le temps de rétablissement le plus court suite à une panne qui affecte le chemin primaire qu'il utilise. QoR_{inf}

indique la classe de plus basse priorité qui ne fournit aucune protection optique particulière au trafic concerné. Le rétablissement de service au trafic de cette classe est délaissé aux soins des couches du niveau supérieur. Les auteurs définissent le temps de rétablissement de la classe QoR_n comme étant $RT(QoR_n) = a + bf(n)$ où a, b et $f(n)$ sont définis par l'administrateur réseau selon l'environnement du réseau. Dans sa plus simple forme, $f(n)$ se définit de la façon suivante : $f(n) = n - 1$. $a = D_{min}$ est le temps de rétablissement minimum incluant le temps nécessaire pour transférer le trafic du chemin primaire (en panne) au chemin de protection. $b = D_{scale}$ inclut le temps de propagation de la panne et la réservation de la bande passante le long du chemin de protection. Arakawa et al. considèrent que pour une topologie donnée, il existe une possibilité de ne trouver aucun chemin de protection capable de garantir un temps de rétablissement maximal comme celui qui est requis par les connexions du chemin primaire. Ce problème est contourné en proposant des classes de fiabilité point à point et non de bout-en-bout. Ainsi, un chemin primaire P est divisé en plusieurs segments et protégé par plusieurs chemins de protections B_x avec $(1 \leq x \leq H)$ où H représente le nombre de sauts du chemin principal. Le temps de rétablissement associé à chaque segment de protection ne dépasse pas une certaine valeur limite. Utilisant cette méthode, le temps de rétablissement maximal associé à P est $RT_{max}(P) = \max RT_x, 1 \leq x \leq B$. First-fit, max-shared et layered-graph sont trois algorithmes heuristiques proposés dans (Arakawa et al., 2003). L'objectif du modèle de conception de topologie logique est de minimiser le nombre de longueurs d'ondes par fibre nécessaires pour le transport du trafic du réseau en respectant les besoins en fiabilité entre chaque pair de noeuds du réseau. Les trois algorithmes classent les paires de noeuds par ordre décroissant en besoin de qualité de fiabilité. Les chemins de protection sont calculés utilisant des algorithmes de plus court chemin et l'assignation de longueurs d'onde est identique sur les deux chemins, principal et de protection. Les résultats montrent que l'algorithme layered-graph est plus performant que les deux autres. Ainsi nous proposons de réduire davantage la bande passante allouée en guise de protection en utilisant des mécanismes des couches supérieures pour accomplir cette tâche.

Les auteurs de (Saradhi et al., 2004) reprennent par la suite la notion de routage dynamique avec protection partielle du trafic initialement proposée dans (Ye et al., 2001). Le concept est de fournir une protection à seulement une fraction α du trafic en cas de panne. Quand une requête de connexion arrive, le routeur périphérique du réseau réserve la capacité nécessaire à la connexion sur un chemin optique primaire. Le processus est répété, mais seulement une fraction α de cette capacité est allouée sur un chemin de protection. Dans le cas d'une panne qui affecte le chemin optique primaire, une portion α du trafic est protégé. En prenant $\alpha = 0.7$, les résultats de simulation du réseau NSF à 14 noeuds montrent que les probabilités de blocage et la quantité de capacité de protection réservée sont de loin inférieures à celles d'un réseau utilisant entièrement une protection 1 :1. Un α différent pour un service différent peut être proposé pour fournir une qualité de protection différenciée.

2.3.8 Une qualité de rétablissement dynamique

Si la différenciation est fournie par des méthodes de restauration dynamique, elle est appelée qualité de rétablissement dynamique. Le paramètre de qualité de service concerné peut être le temps de restauration nécessaire avant que le service ne soit rétabli. Auparavant, la différentiation de service a été établie en fonction de divers paramètres tel l'intervalle de temps séparant l'occurrence de deux pannes, la probabilité de succès de la restauration de service suite à une panne, la probabilité qu'une connexion soit rétablie avec succès, la dégradation de la bande passante et la quantité de trafic restauré suite à une panne. La qualité de rétablissement dynamique se base sur l'utilisation de temps de restauration d'une panne comme paramètre de différenciation.

Lors d'une panne de composante ou fibre optique, plusieurs connexions peuvent être affectées et des demandes de restaurations sont générées simultanément rentrant ainsi en collision. Un service de préemption peut être mis en place pour fournir des services diffé-

renciés en terme de priorité de restauration et de temps de restauration. Les auteurs (Wu and Negi, 2003) expliquent comment la différenciation de service peut être appliquée à la probabilité de restauration réussie ainsi qu'au temps de restauration. Trois politiques de préemption sont ainsi proposées, préemption de restauration (Restauration Preemption (PR)), préemption fonctionnelle (Working Preemption(WP)) et finalement Préemption fonctionnelle de restauration (Restoration and Working Preemption (RWP)).

Dans RP, les tentatives de restauration réalisée par des connexions de haute priorité peuvent préempter les canaux optiques de protection déjà choisis par des connexions de basse priorité forçant ainsi ces dernières à recalculer leurs chemins de protection. Dans WP, les tentatives de restauration réalisée par des connexions de haute priorité peuvent préempter les canaux optiques primaires déjà utilisés par des connexions de basses priorités forçant ces dernières à activer leurs processus de restauration et calculer un chemin secondaire. RWP combine RP et WP. Le choix de la politique dépend intrinsèquement d'une probabilité γ. Le système commence en utilisant RP et si aucun chemin n'est trouvé pour les connexions de haute priorité, WP est utilisé avec une probabilité γ.

2.3.9 Qualité de service différenciée dans les réseaux IP/WDM

Les auteurs de (Saradhi et al., 2004) terminent en proposant GMPLS (Banerjee et al., 2001) pour offrir une qualité de service différenciée, non seulement au niveau WDM mais au niveau IP. Le plan de contrôle de GMPLS permet non seulement la commutation de paquets au niveau IP (LSP) mais aussi au niveau des longueurs d'onde à la couche optique. Ceci permet de transposer les mécanismes de protection différenciée, fiabilité différenciée et restauration différenciée au niveau IP aussi.

2.4 Sommaire

Le but de ce chapitre est d'explorer l'état de l'art et de corroborer la nécessité de la protection différenciée du trafic en cas de panne dans les réseaux de prochaines générations. Nous nous sommes aperçu que la littérature exhibe une certaine constance dans l'utilisation des termes "protection" et "différenciée". Le premier signifie généralement la protection des canaux ou connexions optiques principaux par des canaux secondaires qui sont utilisés seulement comme relève en cas de panne. Le deuxième indique la différenciation de la protection de ces canaux et la littérature démontre une multitude de façons de complexité variée pour s'y prendre. Il est alors clair que pour différencier la protection du trafic en cas de pannes, il faut en premier lieu différencier sa transmission sur des canaux physiques différents et par la suite, différencier la protection de chaque association canal physique/classe de trafic ; ceci est à la base du modèle DiffProtect qui impose, en plus, la séparation sur chemins disjoints des canaux optiques d'un même lien logique.

La littérature nous a par la suite persuadé d'un important consensus dans l'adoption de l'architecture de services différenciés DiffServ comme outil de choix pour différencier la protection du trafic contre la congestion dans la couche logique des réseaux de prochaines générations. Étant donné que l'ultime objectif de ce projet est la proposition d'une technique innovatrice de protection différenciée du trafic en cas de *pannes physiques*, il nous a semblé évident d'explorer la possibilité de réutiliser DiffServ pour la protection du trafic dans ces situations. Surnommée DiffServ*, cette nouvelle pratique nous évite

- le déploiement de deux mesures de protection différenciée, l'une logique contre la congestion et l'autre physique contre les pannes ;
- la complexité et les coûts élevés associée respectivement à la différenciation et la protection du trafic dans la couche physique étant donné qu'il existe un mécanisme logique déjà capable de réaliser ces tâches plus facilement.

Pour éviter de modifier le fonctionnement de DiffServ de façon canonique et sans garantie de réussite, nous avons couplé l'architecture de différenciation de service au concept de routage de connexions optiques par séparation sur chemins disjoints. Ceci permettra, entre autre, qu'une panne physique se manifeste en une congestion dans la couche logique et de laisser DiffServ accomplir sa fonction naturelle.

En somme, nous proposons dans le cadre de ce projet la comparaison de deux modèles de protection différenciée du trafic en cas de pannes. Le plus fidèle à la littérature est DiffProtect et nous le proposons en tant qu'une modèle de protection différencié physique concret et fonctionnel. Suite à une transmission différenciée du trafic dans la couche physique, le modèle DiffProtect protège chaque trafic selon sa priorité en utilisant un des trois niveaux de protection, 1 :1, 1 :N et aucune protection (0 :1). Dans le but de réduire davantage la complexité et les coûts, nous proposons DiffServ* qui est un modèle innovateur qui ne requiert aucun dédoublement de ressources physiques en guise de protection et qui protège le trafic selon sa priorité de façon directe et plus naturelle à la couche logique.

Il est à noter que les deux modèles DiffServ* et DiffProtect sont des techniques de protection de type lien-par-lien et qu'il est possible de les combiner sans le besoin d'aucune coordination de protection particulière entre les couches logiques et physiques. Ceci réduit la complexité de l'implémentation d'une protection, rapide, différenciée et multicouche comme peuvent le requérir nos réseaux actuels. Ce projet propose donc un mécanisme MixProtect de protection multicouche rapide qui ne se base pas sur les mécanismes lents de restauration de la couche IP. Le trafic est immédiatement protégé par DiffProtect sur certains liens logiques, par DiffServ* sur d'autres mais dans aucun des cas, une panne de lien physique n'implique directement une panne de lien logique donc nul besoin des mécanismes de reroutage ; la panne physique est traitée en temps et lieu par le mécanisme en place.

CHAPITRE 3

MÉTHODOLOGIE, SIMULATIONS ET RÉSULTATS

Comme nous l'avons déjà mentionné, la réalisation de ce projet se divise en trois étapes principales. La première consiste en une approche par simulation. Elle permet d'analyser et de comprendre le fonctionnement des modèles DiffServ* et DiffProtect sous différents scénarios de pannes de chemins optiques. La deuxième étape est détaillée dans le chapitre 5 et décrit une implémentation pratique du modèle DiffServ* pour en étudier sa faisabilité et son fonctionnement. La troisième fait l'objet du chapitre 6 et comprend la conception d'un modèle analytique qui permettra de généraliser le déploiement des modèles de protection DiffServ* et DiffProtect pour toute topologie IP/WDM. La section 3.1 décrit les étapes de l'approche par simulation. Les sections suivantes 3.2, 3.3 et 3.4 montrent respectivement les détails et les résultats de simulation d'un réseau de deux noeuds, d'un autre linéaire de quatre noeuds et d'un dernier maillé de 6 noeuds.

3.1 Étude par simulation

L'étude par simulation permet de comparer dans un premier temps les performances des deux modèles et de déterminer leur faisabilité. Cette étape est essentielle pour en comprendre le fonctionnement pratique et pour faire la mise au point sur leur utilisation efficace dans différents réseaux IP/WDM. Chaque modèle réagit différemment à l'occurrence de pannes simples et multiples. La simulation permet de donner un aperçu comparatif de la dégradation de la qualité de service des deux modèles en cas de panne. La simulation permet une évaluation directe de cette dégradation de QdS. Pour ce faire, les taux de perte, les délais et les gigues de chaque type de trafic sont calculés.

Un simulateur bien connu, NS-2, a été utilisé pour simuler les modèles DiffServ* et Diff-Protect. NS-2 n'est conçu que pour simuler des topologies IP. Il permet d'évaluer la performance au niveau IP des trafics. Les modèles DiffServ* et DiffProtect ont été conçus pour réagir aux pannes du niveau optique mais NS-2 est incapable de simuler l'interaction IP-WDM nécessaire. Pour résoudre ce problème, NS-2 a été couplé avec un générateur de pannes. Ce logiciel génère une série de pannes pour chaque lien physique selon les critères suivants :

- la durée de chaque panne est exponentielle et indépendante de la durée de celle précédente et suivante ;
- le temps écoulé entre deux pannes successives est distribué exponentiellement et indépendant des pannes.

Le logiciel traduit ensuite l'effet de ces pannes physiques sur la couche IP par le phénomène de propagation de panne. Avec DiffServ*, la panne d'un canal optique se propage de la couche physique à la couche logique et cause une diminution de la bande passante d'un lien logique. Avec DiffProtect, la propagation de panne d'un canal optique de la couche physique à la couche logique dépend de la technique de protection utilisée pour ce canal et affecte différemment la bande passante allouée à la transmission de chaque classe de trafic. Le logiciel finit par en générer le code TCL (code propre à NS-2) correspondant, ce dernier sera intégré au script de simulation des réseaux considérés. Ainsi, chaque simulation tient compte de la topologie IP, des sources de trafic, et des effets des pannes aléatoires des chemins optiques.

Des traces de simulation de quelques dizaines de Giga-octets ont été créées. Le stockage et la manipulation de ces traces se sont montrés impraticables. Un analyseur de trace en temps réel a été développé pour résoudre ce problème. Ce programme traite les lignes de trace générée par NS-2 au fur et à mesure qu'elles sont générées et renvoie à la fin des simulations les informations suivantes :

- taux de pertes, délais, gigues moyens associés à chaque type de trafic ;

- taux de pertes, délais et gigues de chaque type de trafic dans les différentes situations de pannes ;
- variances et intervalles de confiances des valeurs ci-dessus ;
- distributions des délais et gigues de chaque type de trafic dans les différentes situations de pannes.

3.2 Simulations d'un réseau à deux noeuds

Un réseau à deux noeuds est la plus simple topologie qui puisse être utilisée pour étudier séparément le fonctionnement des modèles DiffServ* et DiffProtect. Les détails de cette étude sont présentés dans ce qui suit.

3.2.1 Simulations avec trafic UDP

Le figure 3.1 montre les topologies IP des modèles DiffServ* et DiffProtect simulées à l'aide de NS-2. Les sources de trafic se chargent de générer les flots de voix, de vidéos et de données. Le noeud EDGE, $E1$, se charge de classifier chaque flot sous sa priorité respective. Pour DiffServ*, les classes sont les suivantes : EF, AF et BE. Quant à DiffProtect, il s'agit des classes de routage et de protection explicite. Dans le cas de DiffServ*, l'effet d'une panne simple ou multiple se traduit par une diminution de bande passante au niveau du lien logique de transmission sur le lien $(C1, C2)$.

La figure 1.10 montrait qu'il existe un lien IP qui relie les routeurs 1 et 2. Les ressources de ce lien sont divisées en trois. Il existera ainsi un sous-lien IP réservé à chaque classe de trafic. NS-2 ne permet pas de connecter deux routeurs IP avec plus d'un lien logique. L'ajout des routeurs intermédiaires entre $C1$ et $C2$ dans le modèle DiffProtect de la figure 3.1 représente simplement un astuce de modélisation. Ainsi, trois chemins IP disjoints, un par

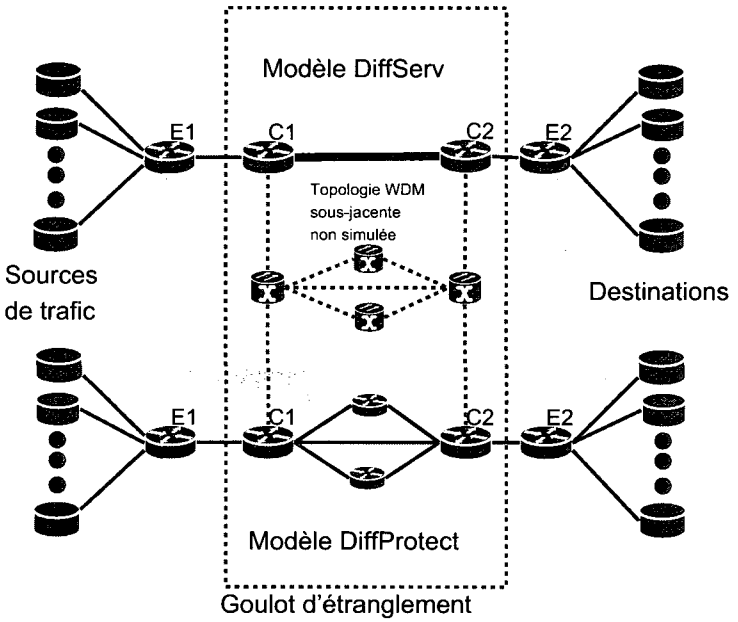


FIG. 3.1 Topologies IP, DiffServ* et DiffProtect, simulées à l'aide de NS-2.

chemin optique et donc par classe de trafic, sont disponibles. Nous avons utilisé le routage explicite pour assigner chaque classe de trafic à un chemin spécifique. Une panne du chemin optique de haute priorité (protection dédiée) n'entraîne aucune conséquence au niveau IP et le trafic EF de cette couche n'est pas affecté. Une panne du chemin de moyenne priorité (protection partielle) entraîne une diminution partielle de la bande passante du chemin IP correspondant. Finalement, la panne du chemin optique de basse priorité (non protégé) cause une panne du chemin IP correspondant.

La simulation des topologies DiffServ* et DiffProtect de la figure 3.1 permet l'évaluation de la performance du sous-réseau à deux noeuds $C1 - C2$. Ces sous-réseaux sont sujets à différents scénarios aléatoires de panne. La performance des mécanismes de protection DiffServ* et DiffProtect peut être ainsi étudiée.

Les résultats de simulation des section suivantes montreront que DiffServ* est un mécanisme IP de protection rapide, qu'il ne requiert aucun surdimensionnement physique et qu'il est capable de protéger adéquatement les trafics de hautes priorités en cas de pannes

simples et, avec certaines limitations, multiples. DiffProtect requiert un dédoublement partiel des ressources physiques et bien que sa performance soit relativement inférieure à celle du modèle DiffServ* en cas de pannes simples, il permet une meilleure protection des flots prioritaires en cas de pannes multiples.

3.2.1.1 Sources de trafic

Dans nos simulations, plusieurs sources de voix sur IP génèrent le trafic de haute priorité. Comme nous l'illustrons à la figure 3.2, chaque source est de type On-Off dans laquelle la longueur d'une période On est distribuée suivant une loi exponentielle de moyenne $1/\mu =$ 400 ms, la longueur d'une période Off est aussi exponentielle de moyenne $1/\lambda = 600$ ms. La source est active durant une période On et génère des paquets de taille fixe de 120 octets à des intervalles fixes de longueur 15 ms. Les périodes Off correspondent aux intervalles durant lesquels la source est silencieuse. Le débit maximal d'une source de voix sur IP est donc de 64 Kbps alors que le débit moyen se maintient à un taux de 25.6 Kbps. Pour éviter la synchronisation des sources, chacune commence par une période Off de longueur aléatoire T_0. Pour évaluer la longueur de ce premier intervalle, un nombre aléatoire p est choisi suivant une distribution uniforme $U(0,1)$. Si $p < P_{On}$ alors $T_0 = 0$ et P_{On} est la probabilité que la source soit dans l'état On. P_{On} est calculé en utilisant l'équation :

$$P_{On} = \frac{1}{1+\mu/\lambda}. \tag{3.1}$$

Si $p > P_{On}$ alors $T_0 \neq 0$ et est évalué en utilisant l'exponentielle de paramètre λ.

Nous utilisons une source de trafic vidéo sur demande pour générer notre trafic de moyenne priorité. Le générateur est basé sur le modèle "Transform Expand Sample (TES)" de plusieurs fichiers traces MPEG-4 (Matrawy et al., 2002). Ce modèle génère du trafic qui possède des statistiques de premier et second ordre identiques à ceux d'une source MPEG-4

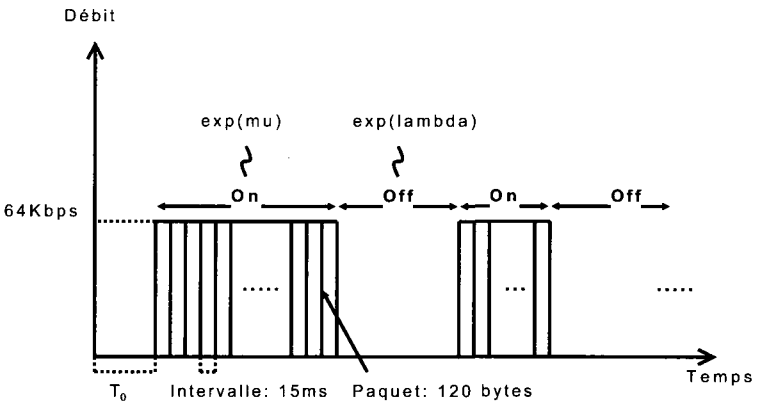


FIG. 3.2 Débit d'une source de VoIP

réelle. La taille des paquets générés est variable et varie entre 100 et 1000 octets. Nous suivons la proposition de (Koucheryavy et al., 2003) en assignant ce type de trafic à la classe AF de l'architecture de DiffServ utilisée.

Finalement, nous utilisons deux sources de trafic UDP pour simuler le trafic de basse priorité. Ce trafic est classifié dans la catégorie BE de l'architecture DiffServ puisqu'il ne requiert pas mieux qu'un service de type meilleur effort. Les sources utilisées dans ce cas sont aussi de types On-Off. Les périodes d'émission de trafic et de veille ont lieu en alternance et sont distribués exponentiellement de moyennes respectives 1 et 0.5 seconde pour la première source et 1.5 et 1 seconde pour la deuxième source. Les deux sources génèrent des grands paquets de taille 1000 octets à des intervalles de 3.2 ms.

Le nombre de sources et leurs caractéristiques ont été choisis de façon à ce que la quantité de trafic généré par chacune soit approximativement la même. Nous utilisons dans nos simulations 75 sources de VoIP, 1 source vidéo et 2 sources de données. La figure 3.3 montre la distribution du débit des sources de voix, nous pouvons voir que le débit moyen est près de 3.39 Mbps alors que le débit maximum a atteint 4.58 Mbps tout en ayant un maximum absolu de 4.8 Mbps quand toutes les sources sont actives simultanément.

La figure 3.4 montre la distribution du débit de la source vidéo de cette simulation. Les

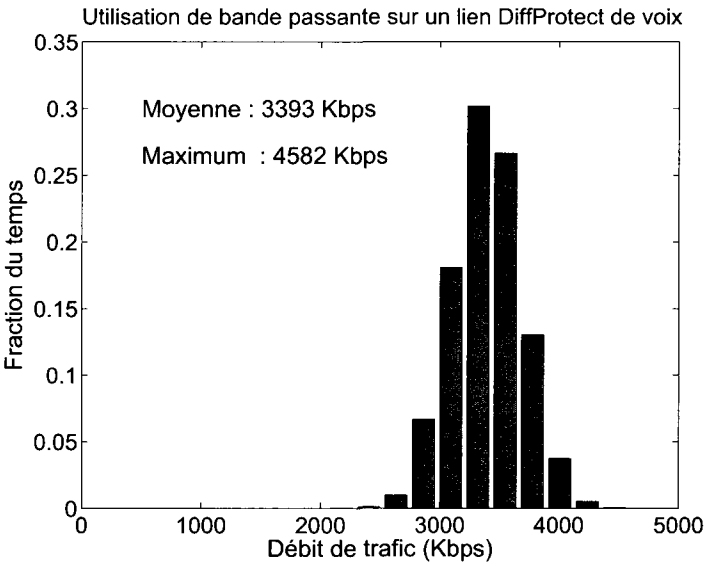


FIG. 3.3 Distribution du trafic de voix sur un lien DiffProtect

paquets générés par cette source sont émis à un taux de 3.08 Mbps, le débit maximum de cette source est de 3.85 Mbps.

Pendant ses périodes d'activité, chaque source de données UDP génère un débit constant de 2.5 Mbps. La figure 3.5 montre la distribution de trafic tel que généré par les deux sources simultanément. Elles génèrent en moyenne 3.16 Mbps de trafic et un débit maximum de 5 Mbps.

Dans nos simulations, chacun des chemins optiques de la figure 3.1 est de 5 Mbps. Vu que le modèle DiffProtect transmet le trafic d'une classe de trafic sur un chemin optique qui lui est propre, une capacité maximale de 5 Mbps est réservée à chaque classe. Puisque le débit maximum pour chaque source de trafic ne dépasse pas 5 Mbps, chaque chemin optique possède assez de capacité pour transmettre la charge qui lui est soumise.

Dans le modèle DiffServ*, les trois chemins optiques qui relient les routeurs 1 et 2 sont regroupés pour former un seul canal de transmission de capacité supérieure de 15 Mbps. Comme dans le cas de DiffProtect, le débit de chaque source ne dépasse pas 5 Mbps et

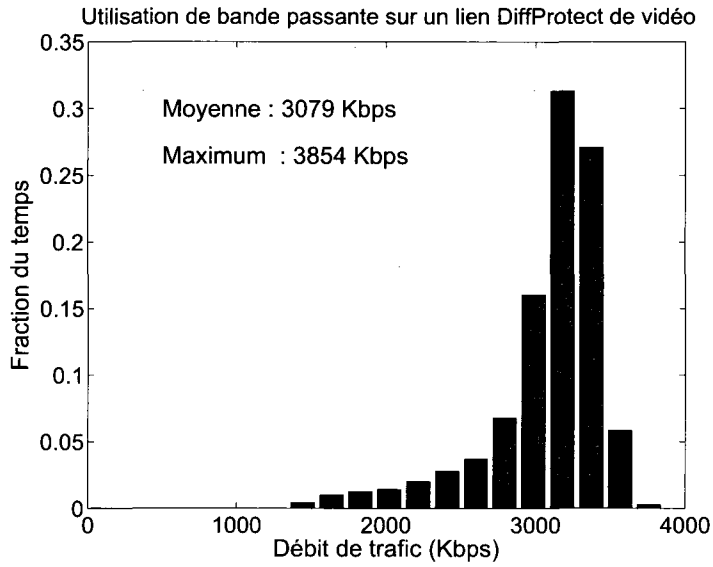


FIG. 3.4 Distribution du trafic vidéo sur un lien DiffProtect

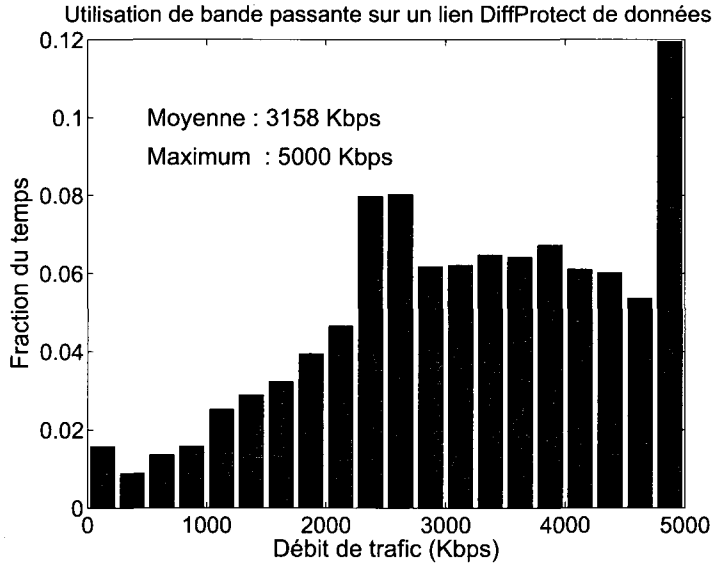


FIG. 3.5 Distribution du trafic de données sur un lien DiffProtect

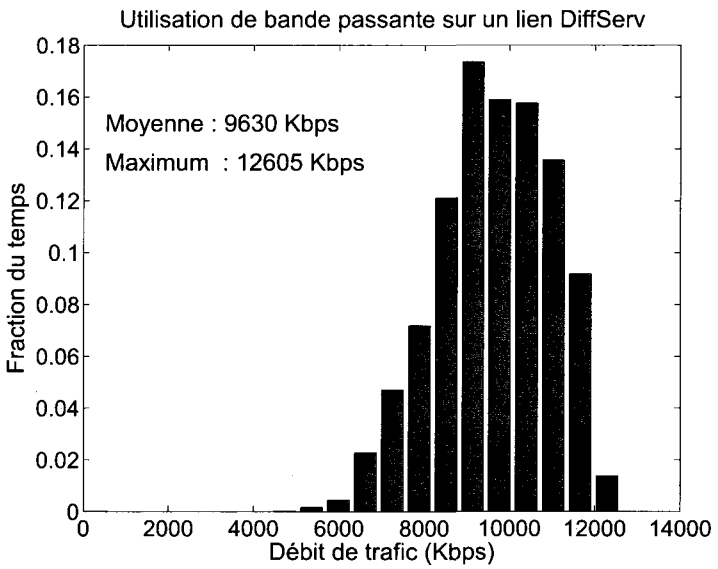


FIG. 3.6 Distribution du débit sur un lien DiffServ*

donc ne requiert pas plus que cette valeur en capacité de transmission. Les trois sources ensemble ne requièrent donc pas plus que 15 Mbps et la discipline d'ordonnancement du modèle DiffServ* a pour effet que chaque trafic recevra approximativement une part égale des 15 Mbps disponibles.

La distribution du débit des trois flots de trafic combinés est montrée dans la figure 3.6. Le débit moyen des sources combinées est évalué à 9.63 Mbps alors que le taux maximal de trafic généré atteint 12.6 Mbps, une valeur qui ne dépasse pas les 15 Mbps de capacité de transmission physique.

3.2.1.2 Détails de simulation et modélisation des pannes

Le but de cette étude est de mesurer la performance du réseau en état de pannes. Ainsi, au cours de chaque simulation, le réseau est soumis à une séquence de configurations de pannes dont chacune est définie comme étant un ensemble aléatoire d'éléments réseaux ou dans ce cas, de chemins optiques en pannes. Pour un petit réseau tel celui simulé dans cette

étude, il est possible d'énumérer toutes les configurations de pannes possibles. Ayant trois chemins optiques qui relient les routeurs $C1$ et $C2$, nous avons une configuration dans laquelle les trois chemins optiques sont fonctionnels, trois avec un chemin en panne, trois autres avec deux chemins en faute et une huitième avec aucun chemin fonctionnel, donc trois en pannes. Avec huit configurations de pannes il est possible de les énumérer et de les simuler une à une pour en étudier la performance du réseau dans chaque cas. Cependant, cette approche est difficilement extensible quand les réseaux deviennent plus grands et complexes. En considérant cette limitation, nous avons décidé d'échantillonner les différentes configurations de pannes possibles et d'en utiliser un sous ensemble aléatoire par simulation.

Dans ce contexte, chaque chemin optique du réseau traverse en alternance une séquence d'intervalles de fonctionnement normal et de panne. Les temps entre les pannes et la durée de ces dernières sont indépendants et distribués exponentiellement. La durée d'un interval de temps de fonctionnement est distribué exponentiellement avec un paramètre $\lambda_{on} = 0.01$. La durée de celle d'un intervalle de panne suit une exponentielle de paramètre $\lambda_{off} = 0.1$. En prenant l'ensemble des trois chemins nous aurons pour chaque simulation un *scénario de pannes* qui est défini par une séquence aléatoire de configurations de pannes simples, doubles, triples et d'intervalles sans pannes.

Une simulation dure 2000 secondes durant laquelle nous recueillons des statistiques sur la performance. À la fin, nous calculons les statistiques de performance pour chaque scénario de pannes qui a eu lieu au cours de la simulation. Au total vingt simulations ont été faites par type de protection (DiffServ* ou DiffProtect), ceci nous a permis d'obtenir des statistiques de performances à des intervalles de confiances de 95%.

Comme mentionné dans la section 3.2.1.1, chaque source de trafic ne requiert pas plus que le tiers de la capacité de transmission totale disponible entre les routeurs 1 et 2 du réseau. Les ressources physiques sont alors adéquatement dimensionnées pour transporter

tous les flots de trafic à leur débit maximum quand il n'y a pas de pannes dans le réseau.

Dans le modèle DiffServ*, la panne d'un ou plusieurs des chemins optiques se traduit par une réduction de la bande passante disponible à la couche IP entre les routeurs $C1$ et $C2$. Comme la capacité de chaque canal optique est de 5 Mbps donc la bande passante IP est réduite d'un tiers, soit de 15 à 10 Mbps. Il n'y aurait congestion que quand le débit de trafic dépasse 10 Mbps soit dans au moins 50% du temps d'après la figure 3.6. Dans cette situation de congestion, les mécanismes de l'architecture DiffServ traitent la congestion en assurant un service prioritaire et adéquat aux classes EF, AF et BE de trafic.

Dans le modèle DiffProtect, chaque trafic est protégé séparément. Le trafic EF n'est jamais affecté par une panne optique puisque son chemin optique est muni d'une protection dédiée. Le chemin IP EF est toujours fonctionnel quelque soit la situation et le trafic EF est toujours et complètement servi en totalité. Le trafic AF n'est affecté par une panne que quand elle a lieu sur le chemin optique qui lui réservé. Nous simulons la protection partielle du chemin optique AF par la réduction de 50% de la capacité du chemin IP correspondant en cas de panne. Nous ne protégeons ainsi qu'une partie du trafic AF en cas de panne. N'étant muni d'aucune forme de protection particulière, la panne du chemin optique BE implique la panne totale du chemin IP BE correspondant. Le trafic BE est ainsi perdu en totalité quand une panne a lieu sur son chemin optique.

3.2.1.3 Performance en cas de pannes

Les résultats de cette section sont publiés dans (Sansò et al., 2006). La simulation des réseaux de la figure 3.1 nous permet d'étudier la performance des modèles DiffServ* et DiffProtect de façon séparée et unitaire. Pour chaque catégorie de trafic nous évaluons :

- le taux de perte de paquets défini comme étant le nombre de paquets perdus sur le nombre total de paquets générés ;

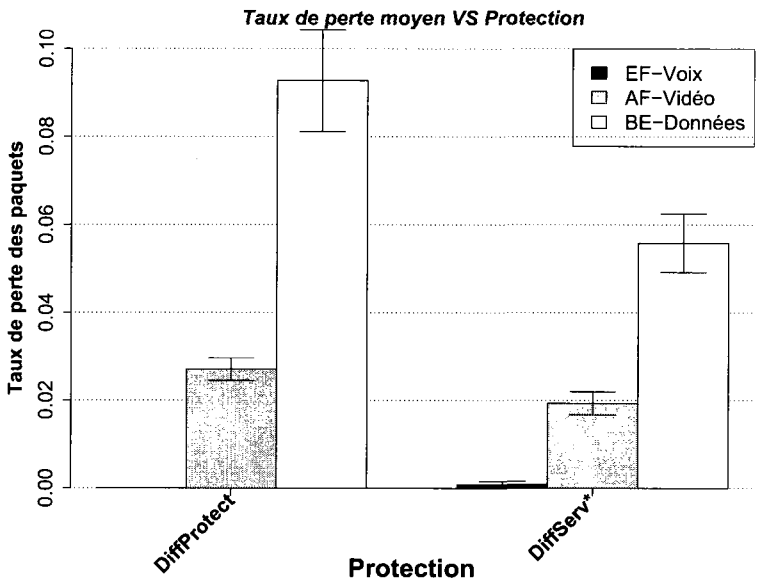


FIG. 3.7 Taux de pertes moyen sous pannes

- le délai moyen par source de trafic calculé comme étant la somme des délais de tous les paquets d'une source divisée par le nombre total de paquets reçus à destination ;
- la gigue moyenne est calculée en utilisant l'équation :

$$\frac{\sum_{i=2}^{n} |d_i - d_{i-1}|}{n-1}$$

le terme d_i est le délai du paquet i, $|d_i - d_{i-1}|$ est la gigue du paquet i.

Le taux de perte, le délai de bout-en-bout et la gigue moyenne pour chaque classe de trafic, chaque modèle de protection et calculés à des intervalles de confiance de 95% sont montrés respectivement dans les figures 3.7, 3.9 et 3.10.

Nous pouvons voir de la figure 3.7 que le trafic EF de voix est presque complètement immunisé contre les pertes dans les deux cas de protection. Dans le cas de DiffProtect, la protection totale du trafic EF est due au chemin de protection dédiée de même capacité que le chemin principal et entièrement réservé à ce trafic en cas de panne. Avec DiffServ*, cette qualité de protection contre les pertes de paquets est un résultat direct de l'ordonnan-

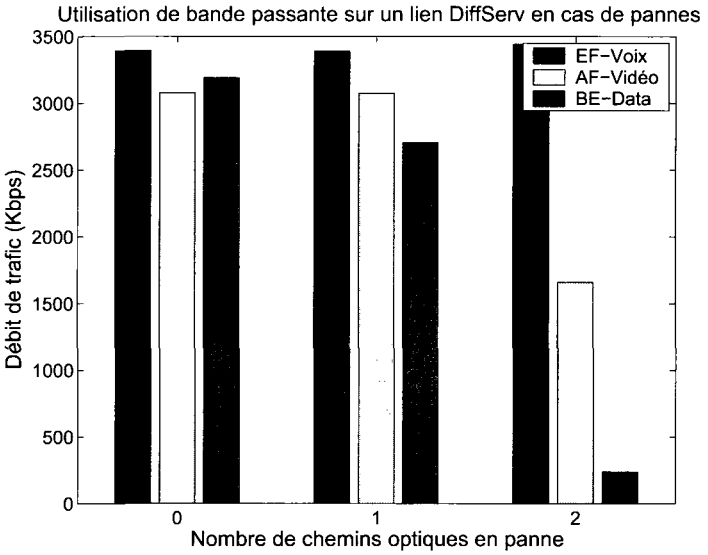


FIG. 3.8 Taux d'utilisation du lien DiffServ* en cas de pannes

cement prioritaire du module DiffServ de ce modèle de protection. Ceci est encore plus visible dans la figure 3.8 qui montre qu'il existe une corrélation directe entre la quantité de bande passante utilisée par chaque catégorie de trafic dans chaque cas de panne avec la priorité de la classe de trafic en question.

En termes de taux de perte des paquets AF et BE nous observons que :

- DiffServ* offre une meilleure performance que DiffProtect ;
- avec DiffProtect, chaque flot utilise un chemin qui lui est propre ;
- en cas de panne(s) dans le modèle DiffProtect :
  - une classe de trafic n'est affectée que par une panne qui touche son propre chemin optique,
  - la protection partielle du chemin AF entraîne automatiquement la perte d'une partie de ce flot,
  - l'absence de la protection du chemin BE mène au rejet de tous les paquets de cette classe,
  - il n'y a aucun partage de ressources, les paquets sont rejetés plutôt que mis en file

d'attente ;

- avec DiffServ*, tous les flots partagent les mêmes ressources de transmission ;
- en cas de panne(s) dans le modèle DiffServ* :
  - la panne de n'importe quel chemin affecte potentiellement toutes les classes,
  - le modèle tend à mettre les paquets en attente au lieu de les rejeter en cas de congestion,
  - les paquets de plus hautes priorités sont servis en premier lieu,
  - les paquets de plus basses priorités sont mis en file d'attente et servis quand la situation le permet,
  - le partage de ressources de DiffServ* assure un taux de rejets plus bas aux flots AF et BE mais des délais d'attentes plus élevés.

La comparaison entre DiffServ* et DiffProtect du délai de bout-en-bout moyen est illustrée dans la figure 3.9. Il est possible de voir que :

- la protection du trafic EF de voix est la même dans les deux cas ;
- les paquets AF ont des meilleures garanties de délais avec DiffServ* qu'avec DiffProtect :
  - avec DiffProtect, la bande passante disponible au trafic AF est celle d'un canal optique et en cas de panne(s) elle est réduite de moitié, les délais AF augmentent,
  - avec DiffServ*, la panne réduit la capacité des ressources de transmission partagées et cette dernière reste supérieure à celle disponible avec DiffProtect*, les délais AF sont plus bas ;
- le délai du trafic de données est plus bas avec DiffProtect qu'avec DiffServ*. Les raisons pour ceci sont :
  - nous calculons le délai seulement pour les paquets qui arrivent à destination,
  - dans le cas de DiffProtect, les taux de perte sont relativement grands,
  - moins de paquets qui arrivent à destination, mais quand il le font, ils arrivent à leur destination plus rapidement.

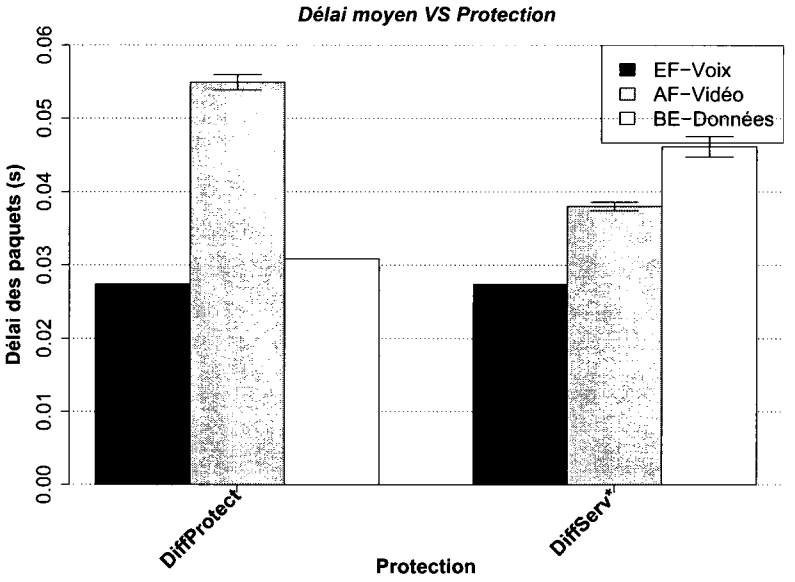


FIG. 3.9 Délai moyen sous pannes

La figure 3.10 montre la gigue moyenne pour le paquets de tout type dans les deux cas de protection :

– la variation du modèle de protection n'affecte pas la gigue des paquets EF de voix ;
– la gigue des paquets AF de vidéo est plus petite avec DiffServ* qu'avec DiffProtect ;
– celle des paquets BE de données est plus grande avec DiffServ* qu'avec DiffProtect.

Dans le cas du trafic AF, nous avons remarqué que la gigue des paquets d'une source qui émet des paquets en rafales est directement liée à la capacité du lien utilisé pour transporter son trafic. Seul un lien avec une grande capacité, tel le cas de DiffServ*, est capable d'assurer une gigue minimale et proche de zéro. Dans le cas de DiffProtect, la classe AF est servie par une portion de la bande passante disponible entre les routeurs 1 et 2. Quand une panne affecte le chemin optique du trafic AF, la capacité du chemin IP correspondant est diminuée de moitié, et ceci résulte en une augmentation dramatique de la gigue du trafic vidéo. Pour une source vidéo comme celle que nous utilisons, les paquets d'une rafale arrivent au routeur 1 pratiquement au même moment. En supposant que les paquets d'une rafale sont servis à tour de rôle et sans interruption, le délai d'attente

d'un paquet quelconque de ce groupe est égal à la somme des temps de service de tous les paquets de la rafale qui sont arrivés avant lui. La différence entre les temps d'attente de deux paquets qui se suivent est égale au temps de transmission d'un paquet vidéo. Cette différence dépend donc de la capacité de transmission du lien utilisé et contribue à la gigue du paquet. Plus la capacité du lien est grande, moindre est la différence, plus petite sera la gigue. À remarquer que la gigue du premier paquet d'une rafale est calculée en fonction du délai de ce paquet qui est le premier du groupe à être servi et le délai du dernier paquet de la rafale précédente, qui est très grand parce qu'il est dernier à être servi, cette différence est d'autant plus petite dans le cas de DiffServ* que DiffProtect.

Remarquons que cette analyse est seulement valide pour des sources de trafic en rafales puisque dans le cas d'une source plus uniforme, les temps d'émissions des paquets sont décalés. Cette différence entre les temps d'arrivée des paquets au routeur 1 donne assez de temps au système pour servir un paquet avant l'arrivée du suivant et le temps d'attente de ce dernier est de ce fait réduit puisqu'à son arrivée le serveur de transmission est déjà libéré.

En ce qui concerne la gigue du trafic de données, le modèle DiffProtect favorise le rejet les paquets BE en cas de pannes au lieu de leur mise en attente. Les paquets BE qui réussissent à traverser un système DiffProtect en état de pannes le font seulement dans le cas où le chemin optique qui leur est dédié est fonctionnel. Ces paquets BE ne subissent aucun temps d'attente supplémentaire, le délai bout-en-bout est minimal pour tous les paquets et la gigue est de ce fait réduite. Dans le cas de DiffServ*, toute panne d'un ou plusieurs chemins optiques réduit la capacité de transmission entre les routeurs 1 et 2. Les conséquences de la congestion résultante sur la performance des paquets BE sont pires à cause de leur basse priorité. Le délai et la gigue de ces paquets sont très grands puisque le taux de service est sévèrement limité par le manque de capacité de transmission et par la quantité de trafic des classes de haute priorité.

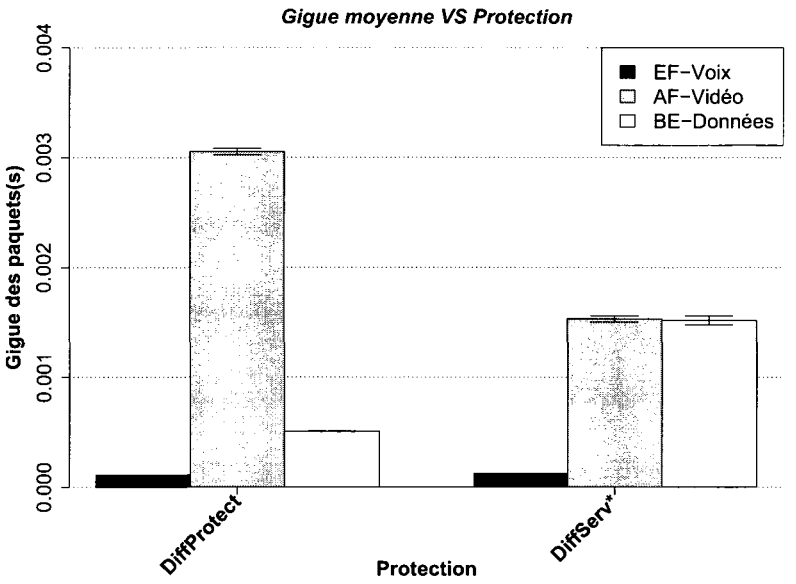


FIG. 3.10 Gigue moyenne sous pannes

En conclusion, nous pouvons déduire des résultats obtenus que les deux modèles de protection peuvent être utilisés pour protéger adéquatement le trafic de voix le plus prioritaire. Le modèle DiffServ* produit une meilleure performance pour le trafic vidéo, surtout en terme de délai et gigue moyenne. Cette amélioration pour la classe AF dans DiffServ* est aux dépends du trafic BE. Bien que le taux de pertes moyen de cette classe de trafic est réduit avec DiffServ*, la dégradation de qualité de service en cas de pannes pour les mesures de délai et gigue est plus importante.

3.2.2 Simulation d'un réseau à deux noeuds et du trafic TCP

Dans ce qui précède, seules des sources qui utilisent le protocole UDP ont été utilisées dans nos simulations. Contrairement à TCP, UDP poursuit l'émission du trafic au même débit configuré quelque soit l'état du réseau et ne fournit aucun mécanisme de retransmission en cas de congestion et de perte de paquets. Le choix d'UDP rend la protection du trafic totalement dépendante des mécanismes DiffServ* et DiffProtect utilisés dans le

réseau. Ces derniers sont étudiés et comparés sous la même charge de trafic dans les deux cas de fonctionnement normal et de panne(s) et sans l'influence d'aucun mécanisme de protection externe, tel TCP par exemple. Les résultats montrés dans la section précédente sont alors évalués dans le pire cas où aucune protection à la source n'est offerte aux flots de trafic et reflètent avec plus d'exactitude la qualité de protection des deux mécanismes proposés.

Une source TCP se base sur un mécanisme qui utilise les accusés de réception comme mécanisme de rétroaction pour déduire l'état du réseau et donc ajuster le débit de trafic en fonction de ce dernier. Dans le cas de nos modèles de simulation, une panne causera une congestion dans le modèle DiffServ* et, si elle touche le chemin optique BE, une perte totale de tous les paquets de cette classe. Une source BE TCP sera en mesure de détecter ces anomalies et réduira de ce fait son débit pour protéger son trafic. Nous aurons ainsi moins de trafic BE qui circule dans le réseau, donc moins de congestion et moins de pertes pour cette classe. Ainsi, TCP peut être considéré comme un mécanisme de protection additionnel qui opère à un niveau supérieur à ceux de DiffServ* et DiffProtect. Le but de cette section est de montrer l'influence de l'utilisation de TCP sur la performance de DiffServ* et DiffProtect en cas de pannes.

Nous réutilisons les mêmes topologies à deux noeuds de la figure 3.1, la seule différence dans ce cas est que les sources UDP de trafic BE sont maintenant remplacées par des sources TCP mais gardent les mêmes caractéristiques de trafic. Les figures 3.11, 3.12 et 3.13 comparent respectivement les valeurs de taux de pertes, les délais et les gigues moyens des différentes classes de trafic. D'après ces résultats, nous pouvons clairement voir que :

- même quand une partie du trafic est TCP, la protection offerte par DiffServ* est toujours meilleure que celle de DiffProtect ;
- les valeurs de délai et gigue dans les simulations sont meilleurs avec TCP qu'avec du

trafic tout UDP ;

- dans les deux cas de DiffProtect et DiffServ*, seule la gigue du trafic BE TCP semble être inférieur que celle du trafic BE UDP ;
- le résultat le plus impressionnant est le taux de pertes des paquets. D'après la figure 3.11 :
  - les flots EF et AF sont protégés de façon similaire avec DiffServ* et DiffProtect,
  - le taux de perte du trafic BE est presque nul.

Ces résultats confirment nos suppositions précédentes qu'une source TCP s'adaptera à la congestion causée par la panne et émettra moins de paquets dans cette situation. La source émet des paquets seulement quand le réseau possède assez de capacité ce qui explique pourquoi les taux de pertes observés ne sont pas significatifs. Il faut noter que la protection offerte à la classe BE qui semble être meilleure que celle de EF et AF dans certains cas n'est pas due à DiffServ* ou à DiffProtect mais bien au protocole TCP qui apporte un supplément de fiabilité quand la situation le requiert.

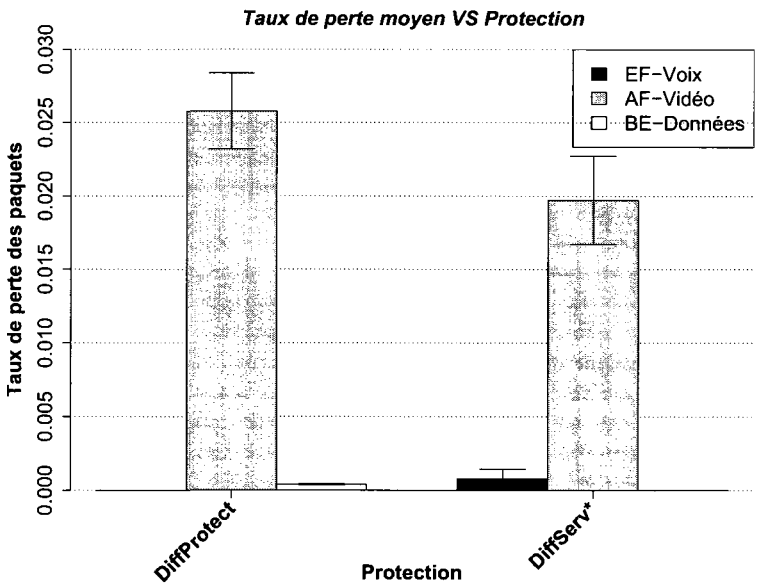


FIG. 3.11 Taux de perte moyen, Trafic BE TCP

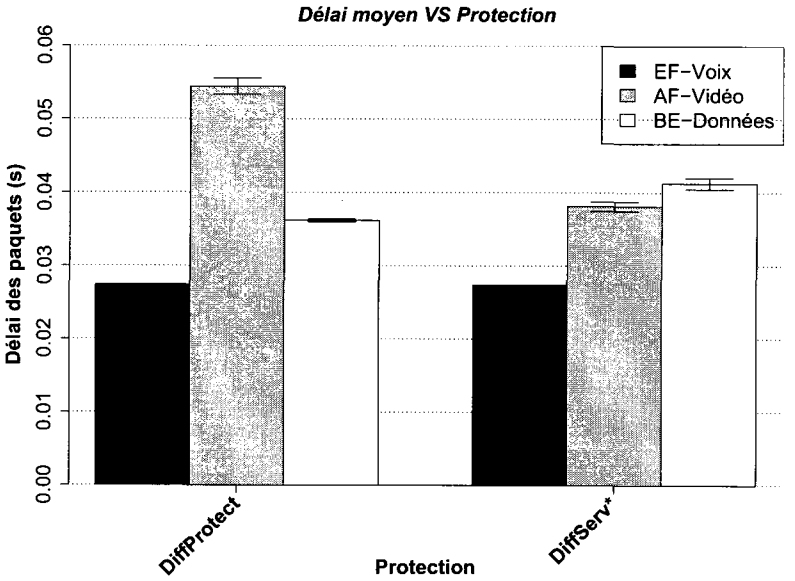


FIG. 3.12 Delai moyen, Trafic BE TCP

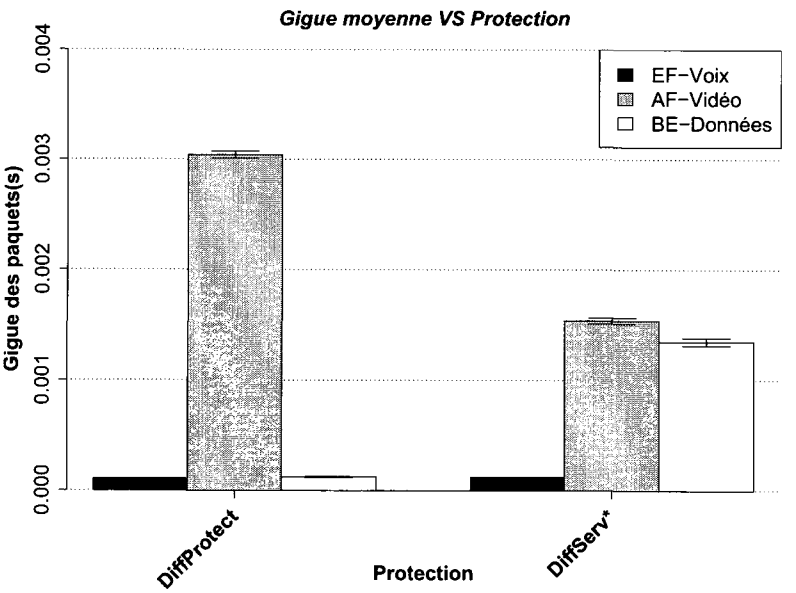


FIG. 3.13 Gigue Moyenne, Trafic BE TCP

3.3 Simulations d'un réseau linéaire à quatre noeuds

La section précédente a permis de comparer de façon directe la performance de DiffServ* à celle de DiffProtect. Les résultats ont permis d'identifier les forces et les faiblesses des deux modèles. Dans ce qui suit, nous étudions un réseau plus grand qui permet de combiner l'utilisation des deux modèles de protection. Dans ce type de réseau, certains liens IP sont protégés par DiffServ* alors que d'autres utilisent DiffProtect. La simulation de tels réseaux permet de combiner les avantages en performance des deux modèles et d'en étudier l'interaction.

Trois liens logiques sont nécessaires pour interconnecter les routeurs d'un réseau linéaire à quatre noeuds. Deux possibilités de protection sont disponibles pour chaque lien. Il existe alors $2^3 = 8$ combinaisons de protection possibles. La méthode par simulation permet de simuler chacune des 8 combinaisons et de trouver celle qui offre les meilleures garanties de qualité de service et qui potentiellement permet de réduire le coût attribué à la redondance optique.

Un réseau qui combine l'utilisation de DiffServ* et DiffProtect est appelé MixProtect. La figure 3.14 montre la version simulée d'un tel réseau. Les flots IP traversent successivement les routeurs 1,2,3 et 4. Le lien $(1, 2)$ est protégé par DiffServ*, $(2, 3)$ par DiffProtect et finalement $(3, 4)$ par DiffServ*, d'où la nomenclature MixProtect DS-DP-DS.

Les résultats de cette section sont publiés dans (Awad et al., 2008) et montrent que l'utilisation croissante de DiffServ* versus DiffProtect dans un tel réseau améliore sa performance moyenne en cas de pannes. Les résultats indiquent par contre que la combinaison DiffServ*-DiffProtect doit être soigneusement choisie pour assurer une qualité de protection maximale aux différents types de trafic. La qualité de protection dépend intrinsèquement du nombre et position des liens protégés par DiffServ* ou DiffProtect et de la nature du trafic injecté dans le réseau, débit constant, On-Off, en rafales, etc.

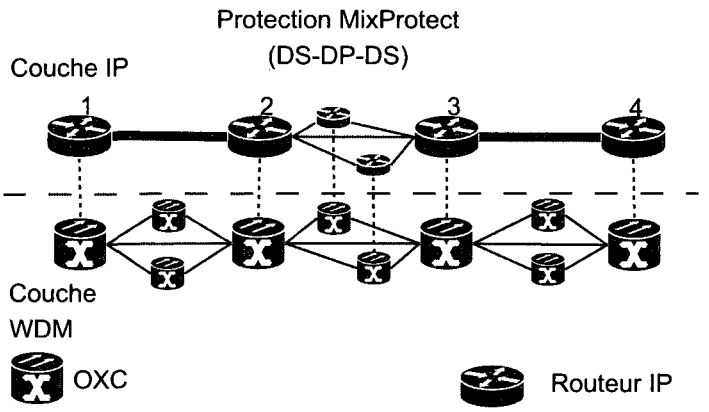


FIG. 3.14 Réseau MixProtect (DS-DP-DS).

3.3.1 Performance moyenne en mode normal

Nous avons d'abord procédé à la simulation des huit combinaisons de protection sans pannes. Pour cette étude, nous utilisons les mêmes modèles DiffServ* et DiffProtect et les mêmes sources *UDP* de trafic de voix, vidéo et de données que ceux décrits à la section 3.2.

Nous évaluons pour chaque simulation le taux moyen de rejet de paquets, le délai moyen de bout-en-bout ainsi que la gigue moyenne par flot et par combinaison de protection. Pour accroître l'exactitude de nos résultats, chaque combinaison de protection a été simulée dix fois. Les valeurs moyennes sont présentées dans les figures 3.15, 3.16 et 3.20. Nous constatons directement que les résultats diffèrent d'une combinaison de protection à l'autre. Bien que les liens de transmission sont adéquatement dimensionnés dans les deux cas de DiffServ* et DiffProtect, la différence réside dans le transfert des paquets dans la couche optique. Dans DiffServ*, la bande passante est partagée entre les différents flots de trafic alors qu'avec DiffProtect, la capacité du lien IP est divisée entre les différents flots et chaque trafic utilise une partie qui lui est réservée de la capacité de transmission totale.

La figure 3.15 montre le taux de perte de paquets pour chaque classe de trafic et pour chaque combinaison de protection. Nous pouvons voir que :

- il n'y a aucune perte de paquets de voix et de données UDP ;
- il y a de faibles pertes, moins de 1%, dans le cas de trafic vidéo ;
- les pertes ont lieu :
  - malgré la simulation sans pannes des réseaux,
  - malgré la priorité des paquets AF qui est plus élevée que celle des paquets BE.

Les sources de trafic vidéo émettent leur trafic en rafales de différentes tailles. Il est possible que le réseau soit incapable de contenir tous les paquets vidéos émis simultanément et soit forcé d'en rejeter quelques un. Des tests effectués subséquemment sur la taille des files d'attentes du réseau ont permis de vérifier cette hypothèse. Nous remarquons que le taux de perte des paquets vidéo est plus élevé quand DiffProtect est utilisé sur tous les liens du réseau que quand au moins un lien est protégé par Diffserv. Ceci est dû au fait que DiffServ* utilise un mécanisme de mise en forme qui assure la conformité d'un trafic à un certain profil prédéfini. Le profil contient des conditions, par exemple, sur le débit de trafic moyen ainsi que la taille maximale d'une rafale. Ce mécanisme est nécessaire parce que dans le cas de DiffServ*, plusieurs trafics partagent les mêmes ressources de transmission. Il est donc important de s'assurer qu'aucun trafic ne dépasse les limites qui lui sont imposées et n'empiète donc pas sur les ressources réservées aux autres flots. Ainsi, si le trafic émis par une source ne respecte pas ce profil, tout excédent est marqué non conforme, voit sa probabilité de rejet augmenter et est rejeté aux premiers signes de problème. DiffProtect est plus efficace dans ce cas puisqu'il assigne au trafic vidéo un chemin de transmission qui lui est réservé de la source jusqu'à la destination.

La graphique de la figure 3.16 montre que le délai moyen du trafic de voix est constant quelle que soit la combinaison de protection utilisée, le trafic EF est toujours assuré d'obtenir la meilleure protection pour tous les MixProtect possibles. Nous pouvons voir aussi

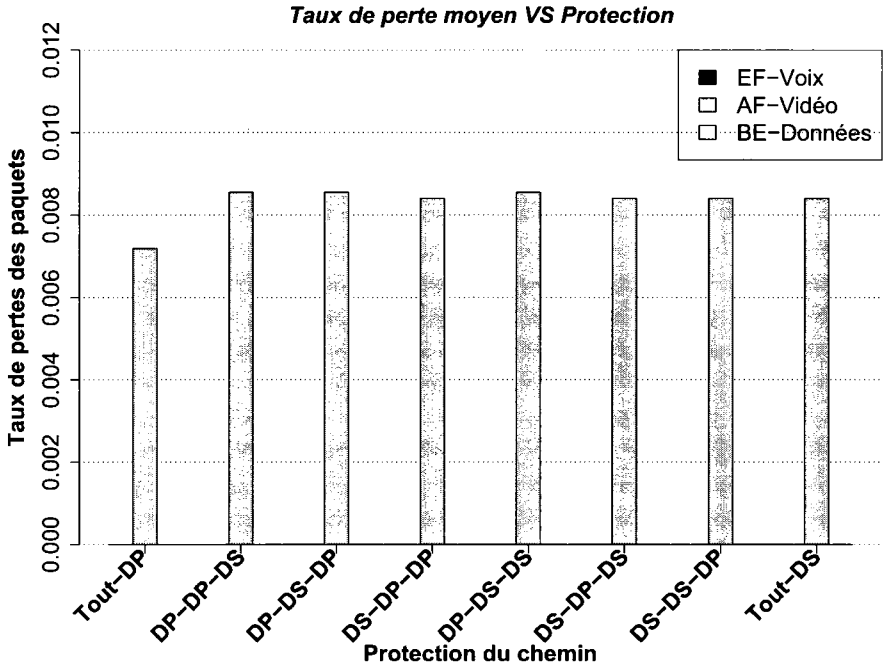


FIG. 3.15 Taux de pertes moyen, sans pannes

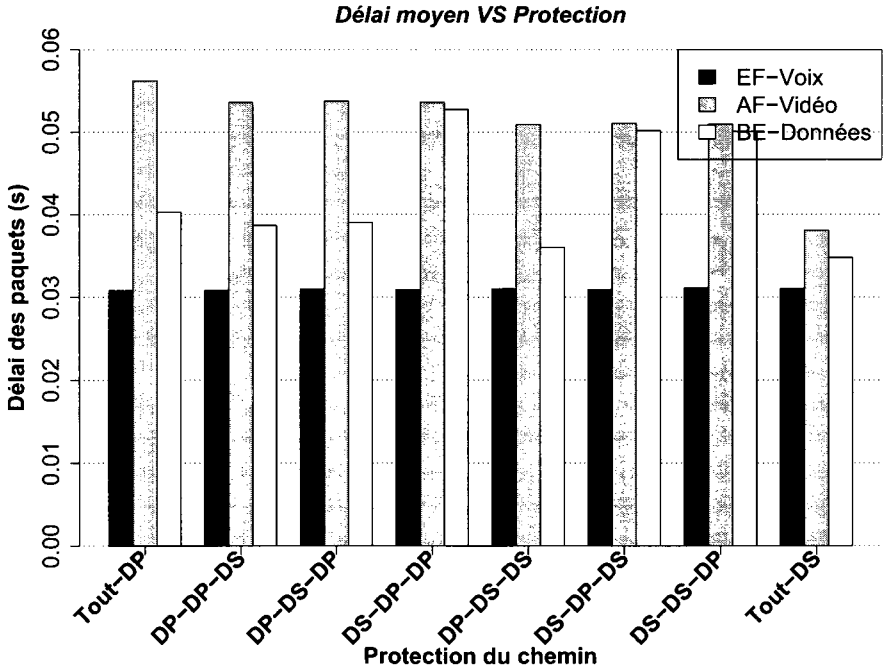


FIG. 3.16 Délai moyen, sans pannes

que le délai moyen du trafic vidéo est réduit quand DiffServ* est utilisé sur un nombre croissant de liens. Le délai de ce trafic est seulement affecté par le nombre de liens qui sont protégés par DiffServ* et non leurs positions respectives sur le chemin utilisé par le flot. Seul un réseau tout-DiffServ* permet de garantir la meilleure performance puisque dans ce cas, la bande passante disponible pour servir le trafic vidéo à chaque partie du chemin est plus grande que celle offerte dans le cas de DiffProtect. En ce qui concerne le trafic de données, la figure 3.16 montre un comportement du délai très différent. En effet, quand DiffServ* est utilisé au point d'entrée du réseau, soit dans les combinaisons DS-DP-DP, DS-DP-DS et DS-DS-DP, le délai du trafic de données augmente pour atteindre le même niveau que le délai du trafic vidéo en rafales. Ce comportement n'est pas observé dans le cas DS-DS-DS dans lequel DiffServ* est à l'entrée du réseau, il est déployé sur tous les autres liens du chemin et le délai BE est à son plus bas niveau. Ceci nous permet de conclure que la position de DiffServ* à l'entrée du réseau est une condition nécessaire, mais non suffisante puisqu'il est aussi nécessaire d'avoir DiffProtect sur au moins un lien subséquent du réseau pour observer la dégradation de performance mentionnée. Ainsi, nous pouvons déduire que le délai du trafic BE est grandement affecté par le changement de DiffServ* à DiffProtect le long d'un chemin donné et que la position relative des techniques de protection aura une grande influence sur la performance.

Une analyse plus raffinée des effets de la combinaison de protection sur le délai est montrée dans les figures 3.17, 3.18 et 3.19. Chacune de ces figures montre le délai moyen par classe de trafic sur chacun des trois liens du réseau. La figure 3.17 montre le délai moyen de paquets sur le lien qui relie les routeurs 1 et 2. Quand ce lien est protégé par DiffProtect, le délai moyen des paquets vidéo est deux fois plus grand que celui observé quand ce même lien est protégé par DiffServ*. Ceci est une conséquence directe de la capacité de transmission mise à la disposition du trafic vidéo en rafales à l'entrée su réseau. Avec DiffServ*, la capacité de transmission du lien à l'entrée du réseau est plus grande, ceci implique que le temps de service des paquets d'une rafale vidéo sera plus faible que quand

ces derniers doivent utiliser seulement une portion de la bande passante disponible comme dans le cas de DiffProtect. La variation de la protection du premier lien n'affecte pas la performance du trafic EF et a un impact mineur sur les flots BE de données, les flots de voix et données n'étant pas émis en rafales.

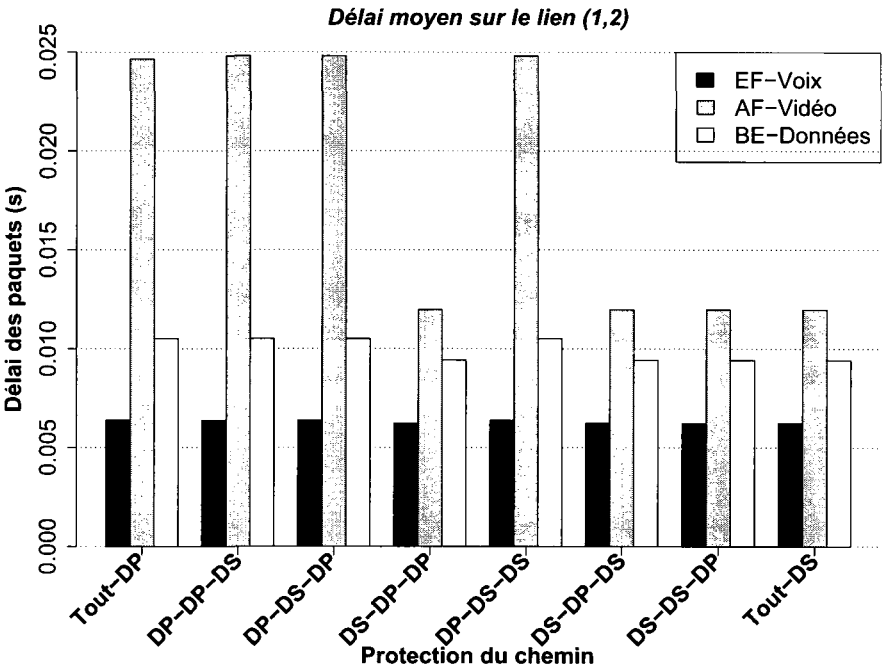


FIG. 3.17 Délai sur le lien (1,2)

La figure 3.18 montre le délai encouru par les différents flots de trafic au lien $(2,3)$ du réseau. Les résultats montrent que :

- la technique de protection de ce lien n'a aucun effet sur le délai de la classe EF ;
- le délai des flots AF et BE est à son maximum quand :
  - le lien $(2,3)$ est protégé par DiffProtect,
  - le lien précédent $(1,2)$ est protégé par DiffServ*.

Nous expliquons ceci par le fait que chacun des flots vidéo et données passe d'un lien à haute capacité, DiffServ*, à un sous-lien DiffProtect de plus basse vitesse. Les délais sont plus grands puisque les paquets AF et BE arrivent au routeur 2 à une vitesse plus grande

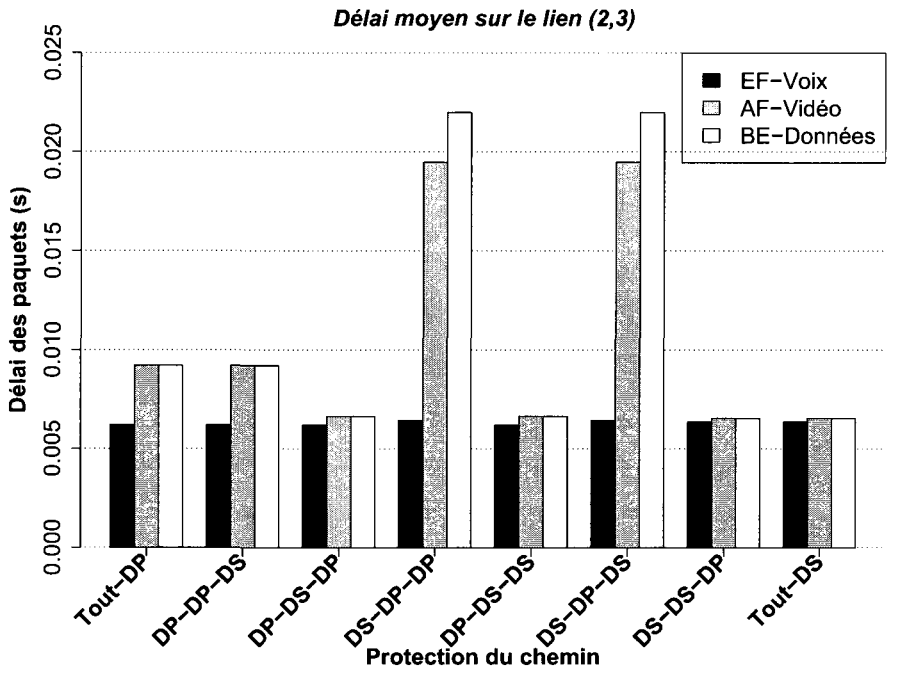


FIG. 3.18 Délai sur le lien (2,3)

que celle avec laquelle ils peuvent quitter ce noeud sur les canaux optiques qui leur sont réservés dans le lien $(2,3)$. Cette transition n'a pas le même impact sur les paquets de voix puisqu'ils sont de haute priorité et de taille plus petite et donc moins affectés par le changement de capacité de transmission.

Finalement, la figure 3.19 montre les délais encourus sur le dernier lien du réseau. Comme dans le cas du lien $(2,3)$, nous avons que :

- le délai des flots AF et BE est plus important quand une transition de DiffServ* à DiffProtect a lieu ;
- ces délais atteignent leur maximum quand les paquets traversent une portion tout-DiffServ* du chemin avant d'arriver à un lien DiffProtect.

Le comportement de la gigue est étudié dans la figure 3.20. Les résultats montrent que :

- la gigue des paquets de voix augmente faiblement avec le nombre de liens protégés par DiffServ* ;

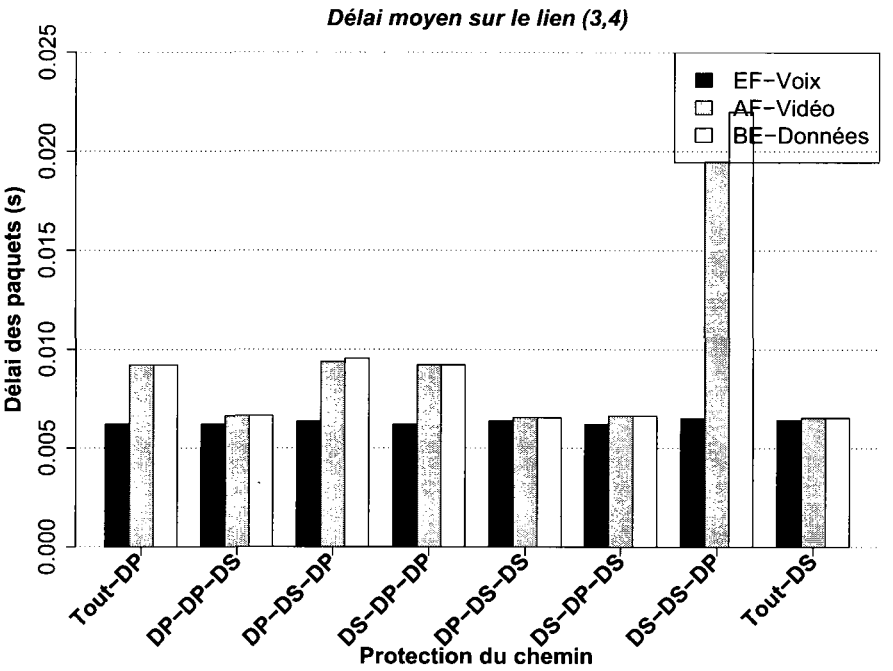


FIG. 3.19 Délai sur le lien (3,4)

- un nombre croissant de liens protégés par DiffServ* diminue la gigue des paquets vidéo AF ;
- la gigue du trafic BE augmente quand plus de liens sont protégés par DiffServ*.

La gigue de la classe AF est pratiquement le double quand au moins un lien est protégé par DiffProtect. Encore une fois, DiffProtect divise la capacité de transmission disponible au niveau physique entre les trois classes de trafic. Ceci implique que les paquets AF sont servis par un lien de plus faible capacité. Étant donné la nature en rafale de ce flot, la gigue sera d'autant plus importante. La situation est inverse avec DiffServ*, une plus grande capacité de transmission assure un service beaucoup plus rapide aux paquets AF et permet alors d'obtenir des valeurs de délai et de gigue plus faibles pour cette classe. Le figure 3.20 montre aussi que la gigue des paquets BE est plus grande quand DiffServ* est utilisé à l'entrée du réseau. Cette observation est une autre indication que la position des mécanismes de protection est un facteur important qui peut affecter la performance.

Dans le réseau tout-DiffServ*, la gigue des paquets BE atteint son maximum en raison de la faible priorité de ces derniers dans l'accès du lien protégé par DiffServ*.

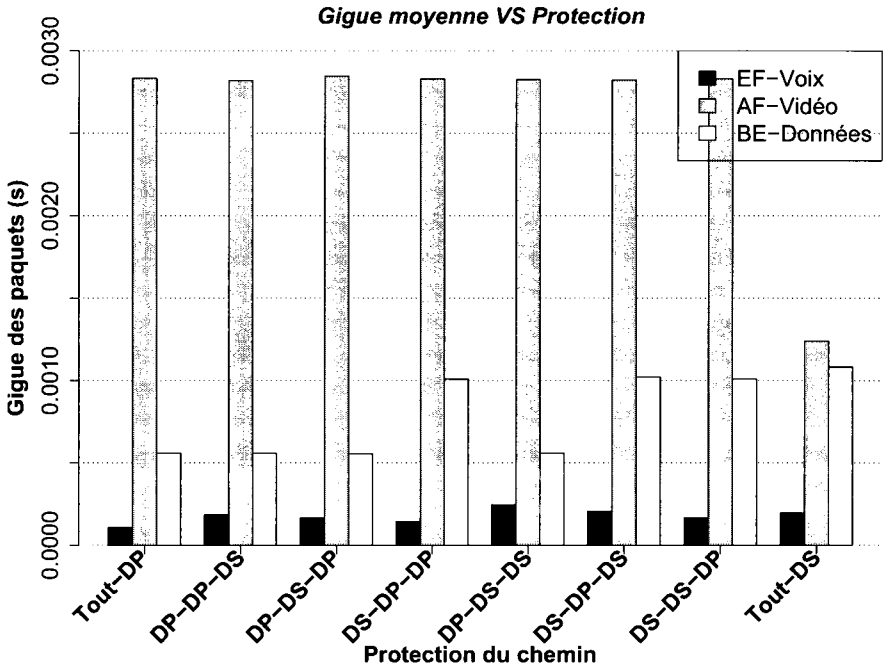


FIG. 3.20 Gigue moyenne, sans pannes

3.3.2 Performance moyenne en cas de pannes

Nous simulons pour cette étude les huit combinaisons de protection DiffServ*/DiffProtect possibles pour le réseau linéaire à quatre noeuds. Nous étudions la fiabilité de chaque combinaison et nous essayons d'identifier la combinaison qui offre la meilleure protection pour chaque classe de trafic et chaque mesure de performance. Nous simulons les combinaisons tout-DiffServ*, tout-DiffProtect et les six MixProtect sous différents scénarios de pannes. La génération des pannes se fait indépendamment pour chaque chemin optique d'un lien logique et pour chaque lien logique du réseau considéré. Comme dans le cas du réseau à deux noeuds, la durée des pannes et des temps inter-pannes de chaque chemin optique sont tout deux distribués exponentiellement. La durée moyenne d'une panne est

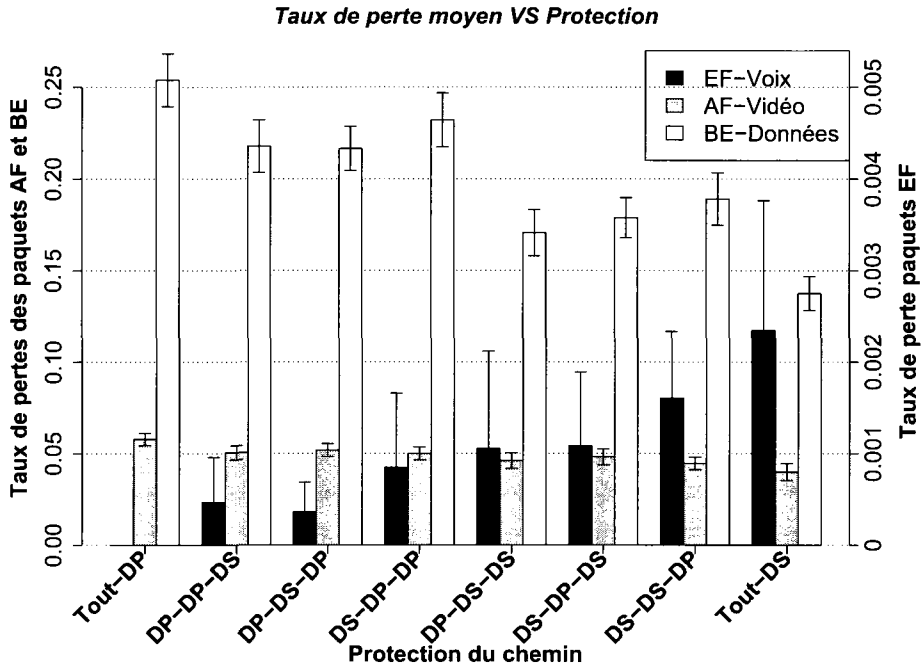


FIG. 3.21 Taux de pertes moyen, avec pannes

de 10 secondes, celle de l'intervalle entre deux pannes successives est de 100 secondes. Les chemins optiques tombent en panne indépendamment les uns des autres, ceci permet d'avoir en alternance et dans n'importe quel ordre pour chaque lien logique des séquences de pannes simples, doubles, triples et des périodes sans aucune panne. Vu que le réseau est composé de trois liens, la panne la plus sévère qui touche ces derniers détermine l'état du réseau. Ainsi, si le premier lien du réseau est en panne simple, le deuxième est en panne double et le troisième fonctionne normalement, nous disons que le réseau est en état de panne double. À titre indicatif nous montrons dans le tableau 3.1 le nombre moyen de configurations de pannes simples, doubles, triples et aucune qui affecte chaque lien individuellement et le réseau entier pendant une simulation de 2000s. Les résultats montrent qu'en moyenne, 100 pannes simples, 15 pannes doubles et 1 panne triple affectent chaque lien logique du réseau. Le nombre de fois que le réseau est en état de panne simple est de 205, 44 pour l'état de panne double et 2 pour l'état de panne triple. Bien que la fréquence élevée des pannes ne reflète pas une situation réelle, elle est justifiée par nos besoins

	Lien logique 1	Lien logique 2	Lien logique 3	Réseau
Panne simple	102.28	103.2	104.32	205.36
Panne double	13.2	16.24	16.16	44.4
Panne triple	0.84	0.72	0.72	2.28

TAB. 3.1 Nombre moyen de configurations de pannes qui affectent les liens logiques et le réseau

d'échantillonner les différents états de pannes possibles au cours de chaque simulation.

Sous l'effet des pannes, nous mesurons les moyennes de taux de perte de paquets, de délai de bout-en-bout et de gigue pour chaque classe de trafic et pour chaque combinaison de protection. Un tracé des taux de perte de chaque classe de trafic en fonction des combinaisons de protection est montré à la figure 3.21. Étant donné qu'il y a une grande différence entre les taux de perte des classes AF et BE et celle de EF, nous traçons cette dernière en utilisant l'échelle de l'axe des ordonnées Y à droite du graphique, les résultats AF et BE sont tracés en concordance avec l'échelle la plus grande de l'axe Y à gauche. Cette technique montre avec plus de détails l'effet de la variation de protection sur le taux de perte des paquets EF.

La figure 3.21 montre que :

- à cause de sa faible priorité, le trafic BE subit le plus grand taux de perte ;
- le taux de perte AF est très inférieur à celui de BE ;
- le trafic EF bénéficie d'une protection proche de 99.9% ;
- un nombre croissant de liens protégés par DiffServ* diminue les taux de perte des classes AF et BE.

Ceci montre encore l'avantage de DiffServ* qui permet le partage d'un lien de grande capacité entre différentes classes de trafic par rapport à DiffProtect qui divise la capacité de transmission de façon stricte et réserve des liens de capacité plus faibles à chaque classe individuellement.

Le délai des différents flots de trafic est montré dans la figure 3.22 où nous voyons que

quand DiffServ* devient la forme principale de protection dans le réseau :

- le délai des paquets de voix augmente faiblement ;
- le délai diminue de moitié pour les paquets de vidéo ;
- le délai moyen des paquets BE est double par rapport au cas tout-DiffProtect.

Dans le cas de DiffProtect, les pannes du niveau physique n'ont aucun effet sur la performance du trafic EF. Quelle que soit la situation, ce modèle a toujours un chemin optique de capacité garantie qui lui est réservé. Dans le cas de DiffServ*, toute panne au niveau physique se propage en tant qu'une diminution de la capacité de transmission totale disponible au niveau IP. Vu que nous utilisons un mécanisme d'ordonnancement prioritaire sans préemption au niveau de DiffServ*, les paquets EF ont toujours priorité absolue, mais seulement dans le cas où le serveur est libre. Si un paquet EF arrive alors qu'un autre paquet de plus basse priorité est déjà en service, le paquet devra attendre la fin du service de ce dernier avant qu'il ne soit transmis. Si la capacité de transmission est diminuée à cause d'une panne, le temps de transmission du paquet de basse priorité est plus long alors le délai d'attente du paquet EF sera allongé d'autant. Ceci explique la légère croissance du délai du trafic EF quand DiffServ* devient la forme de protection dominante dans le réseau.

Dans le cas du trafic vidéo, la figure montre que le délai décroit avec l'utilisation croissante de DiffServ* dans le réseau et ce délai atteint son minimum dans le cas du réseau tout-DiffServ*. Pour les mêmes raisons évoquées dans le cas du réseau à deux noeuds, l'évolution décroissante du délai vidéo est due à la disponibilité d'une capacité de transmission plus grande et plus adaptée à un trafic en rafales.

Nous savons que la tendance de DiffProtect est de rejeter les paquets de données en cas de pannes. Dans ces conditions, le délai moyen des paquets survivants est moindre avec DiffProtect qu'avec DiffServ* qui a la tendance de mettre les paquets de faibles priorités en attente en cas de problèmes.

Si nous comparons les résultats de la figure 3.21 avec ceux de la figure 3.16 en fonctionnement normal, nous pouvons voir l'effet des pannes et de la combinaison de protection sur la dégradation du délai pour les trois classes de trafic. Nous pouvons observer que :

- il est évident que le délai du trafic de voix est le même en cas de pannes ou non ;
- le délai vidéo est plus grand en cas de pannes cependant :
  - nous distinguons une évolution similaire de ce dernier dans les deux situations,
  - le délai vidéo décroit quand l'utilisation de DiffServ* augmente,
  - seulement un réseau tout-DiffServ* garantit à ce trafic le même niveau de performance en fonctionnement normal et en cas de panne,
- le comportement du délai du trafic BE est différent en cas de panne, ce dernier augmente quand DiffServ* devient prédominant.

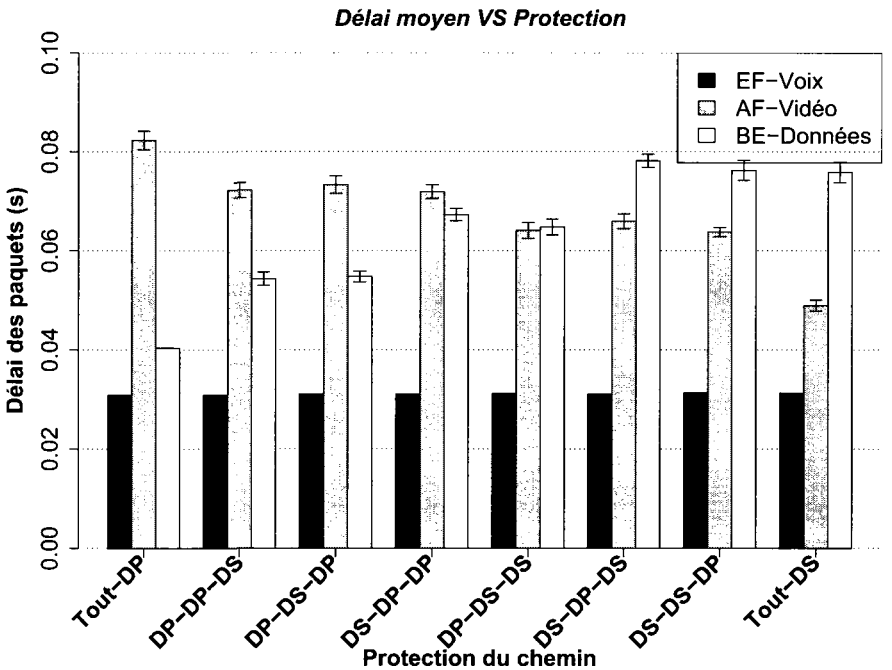


FIG. 3.22 Délai moyen, avec pannes

La figure 3.23 montre que l'utilisation croissante de DiffServ* :

- augmente de façon négligeable la gique du trafic EF ;
- diminue la gigue de la classe AF et même si DiffServ* est utilisé plus fréquemment :
  - l'utilisation de DiffProtect sur au moins un lien du réseau double la gigue AF ;

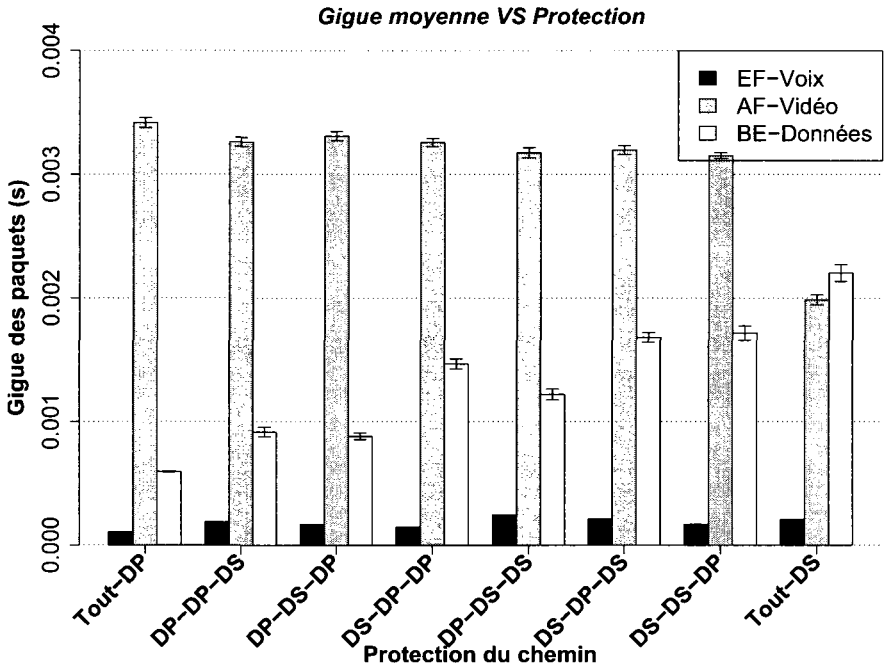


FIG. 3.23 Gigue moyenne, avec pannes

- la gigue du trafic BE augmente :
  - en comparant le cas tout-DiffProtect à tout-DiffServ*, la gigue BE est quadruple.

3.3.3 Distributions de performance en cas de pannes

Dans la section 3.3.2 nous avons analysé les valeurs moyennes du taux de pertes, de délai de bout-en-bout et de gigue pour chaque classe de trafic. Ce type d'analyse ne donne qu'une vue générale sur le comportement du réseau en cas de pannes. Une analyse supplémentaire des distributions des mesures de performance est présentée dans cette section. Elle donne plus de détails sur l'effet des différentes pannes sur la performance du réseau perçue par chaque flot individuellement.

3.3.3.1 Distributions de performance de voix et de données

Nous analysons les distributions du délai et de gigue pour chaque combinaison de protection, chaque classe de trafic et dans les états d'aucune panne, panne simple et panne double. L'énumération totale résulte en un total de 144 graphiques (c.f. l'annexe II). Nous résumons donc les résultats pour le trafic de voix et de données, seules les distributions les plus intéressantes, celles du délai pour le trafic vidéo en cas de pannes doubles sont montrées et analysées en détail.

Quand le nombre de liens protégés par DiffServ* augmente, nous observons que les distributions de délai et de gigue du trafic de voix sont légèrement plus dispersées. Étant donné que les différences sont tellement minimes, nous pouvons dire que la performance est toujours garantie pour le trafic de voix dans toute situation de panne et avec toute combinaison de protection.

Dans un réseau tout-DiffProtect, le flot BE utilise un chemin optique qui lui est propre de l'origine à la destination. Quand le réseau est en état de panne, le flot BE n'est affecté que quand la panne est sur le chemin qu'il utilise. Dans tout autre cas, le service au trafic de données demeure ininterrompu. Ceci résulte en un taux de perte plus élevé, mais des distributions de délai et de gigue étroites et limitées. Le comportement inverse est observé quand le nombre de liens qui utilisent DiffServ* augmente. En cas de pannes, le modèle DiffServ* met plus de paquets en attente, les valeurs de délai et de gigue sont de ce fait plus élevées que celles observées quand le réseau est entièrement protégé par DiffProtect. Ce dernier protège le trafic de données contre des valeurs élevées de délai et de gigue, mais rejette plus de paquets de basse priorité.

3.3.3.2 Distributions de performance de vidéo

Aucune différence significative de performance de délai et de gigue AF n'a été observée entre les huit combinaisons de protection en cas de fonctionnement normal et de pannes simples. Les résultats de performance du trafic vidéo sont résumés ci-dessous :

- en cas d'opération normale et quand DiffServ* devient prédominant dans le réseau :
  - les résultats de délais sont similaires à des distributions exponentielles tronquées ;
- en cas de pannes simples,
  - seul un réseau tout-DiffServ* préserve la distribution de délai sous forme exponentielle,
  - les autres combinaisons de protection entrainent des distributions de type bimodal.

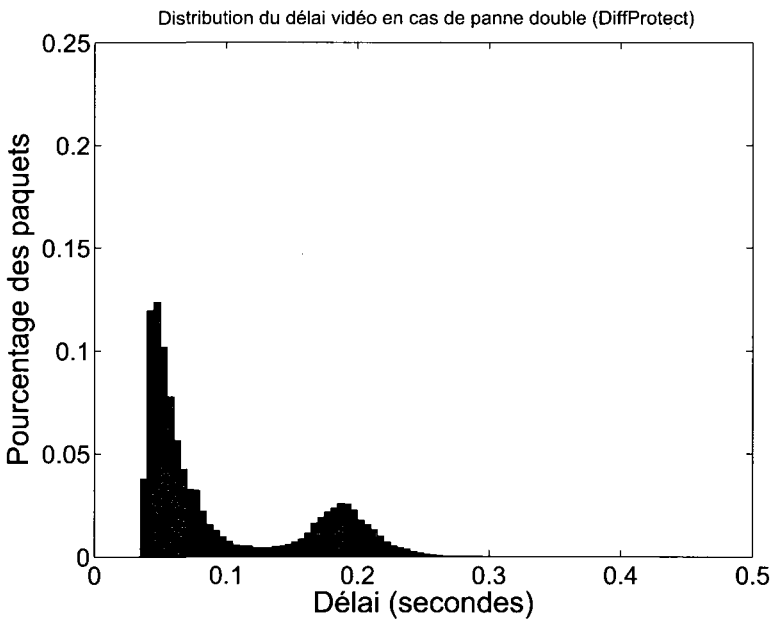


FIG. 3.24 FDP du délai avec DP-DP-DP

Les résultats en cas de pannes doubles montrent par contre un comportement différent. Les figures 3.24 à 3.31 montrent l'effet de l'usage additionnel de DiffServ* sur les distributions de délai vidéo en cas de pannes doubles. Cet effet est différent d'une combinaison

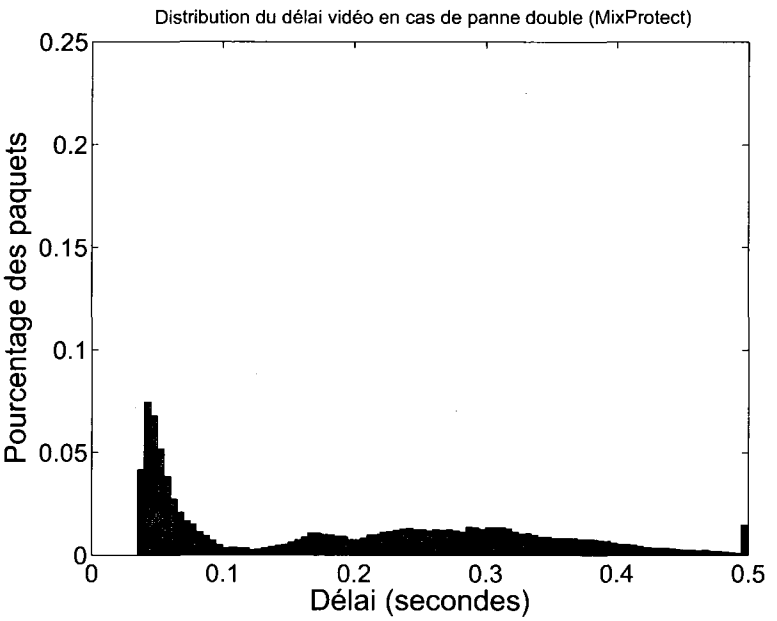


FIG. 3.25 FDP du délai avec DP-DP-DS

de protection à l'autre et ceci est reflété dans les histogrammes de performance qui sont discutés prochainement.

Pour un lien protégé par DiffServ* et composé de trois chemins optiques de même capacité, une panne double peut avoir lieu sur le premier et le deuxième chemin, le deuxième et le troisième ou bien le premier et le troisième. Quelle que soit la position de la panne double, le même effet est observé au niveau IP, la bande passante du lien logique est diminuée au tiers de sa valeur originale, toutes les classes sont affectées par la congestion qui en résulte et la performance par classe dépend seulement de sa priorité de service. La situation est différente dans le cas de DiffProtect. Une panne double peut avoir lieu sur les chemins EF et BE sans toucher le chemin réservé au trafic AF. Dans ce cas, la performance en cas de pannes pour un flot donné dépend non seulement de sa priorité et de la protection qui lui est offerte, mais aussi de la position de la panne dans le réseau.

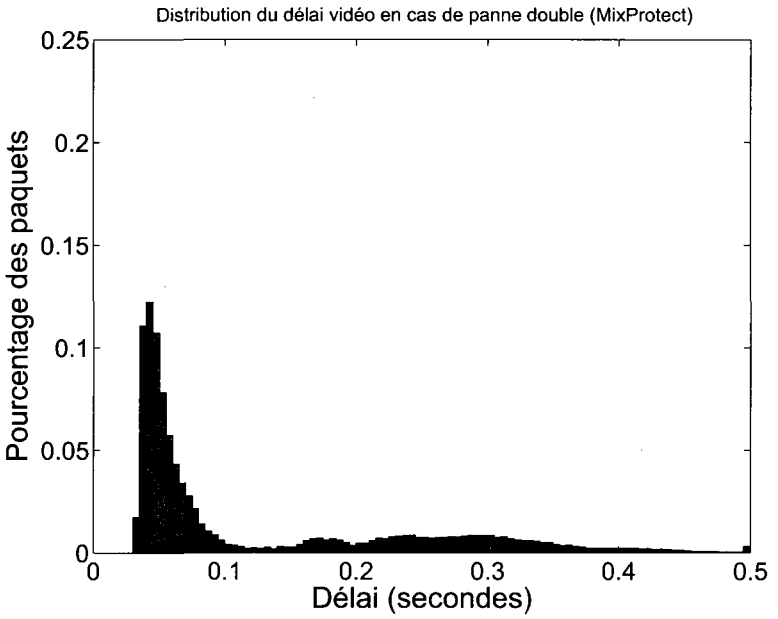


FIG. 3.26 FDP du délai avec DP-DS-DS

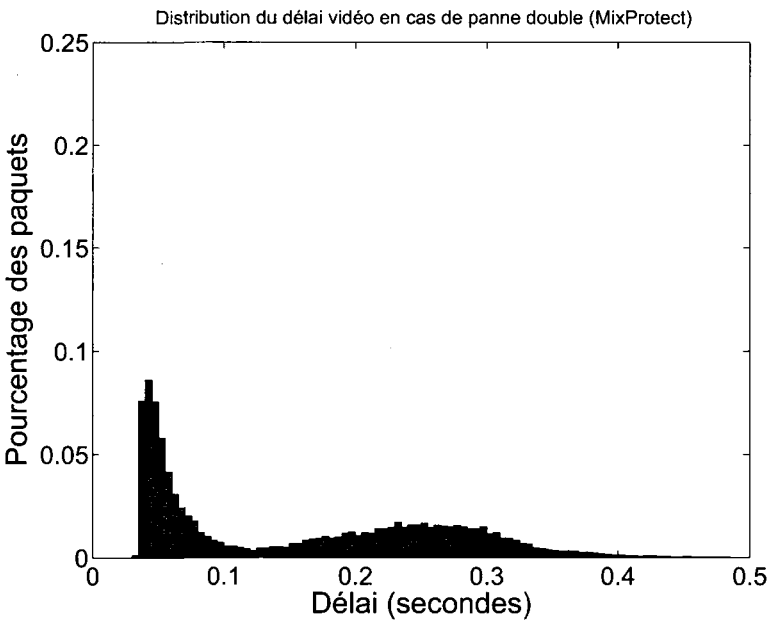


FIG. 3.27 FDP du délai avec DS-DP-DS

La position variable d'une panne double dans le cas de DiffProtect explique la forme bimodale de la distribution du délai de la figure 3.24. Quand une panne touche les chemins optiques de voix et de données, le trafic vidéo n'est pas affecté et est transmis dans un délai minimal. Quand une panne touche le chemin optique vidéo, sa bande passante est réduite de 50%, le délai de transmission des paquets ainsi que leurs temps d'attentes sont plus grands. Ceci explique la formation du second sommet dans la distribution du délai. D'autres résultats montrent que la hauteur du second sommet est plus grande quand la fréquence de pannes doubles qui affecte le chemin optique vidéo augmente.

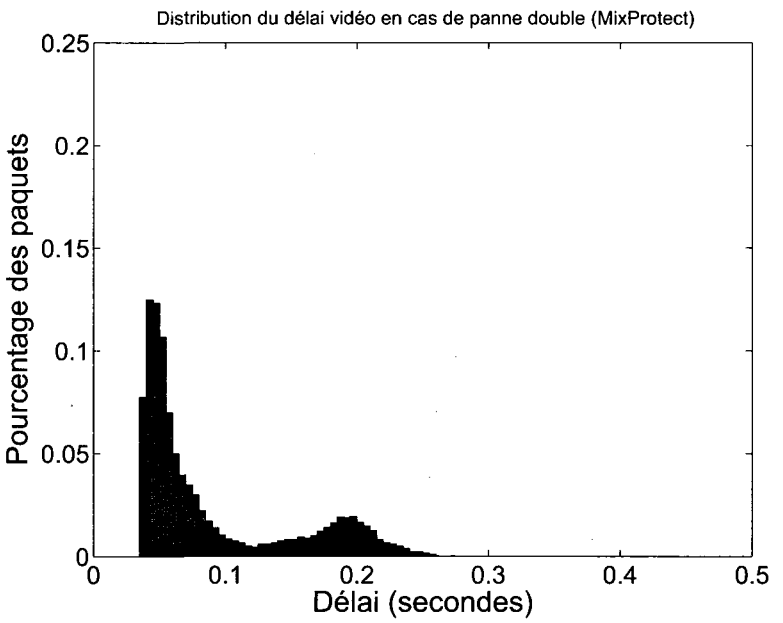


FIG. 3.28 FDP du délai avec DP-DS-DP

Les figures 3.25, 3.26, et 3.27 montrent respectivement les distributions du délai pour les combinaisons de protection qui se terminent par DS : DP-DP-DS, DP-DS-DS et DS-DP-DS. Étant tous similaires, nous pouvons voir que l'utilisation de DiffServ* au point de sortie du réseau étale le second sommet jusqu'à des valeurs de plus de 500 ms.

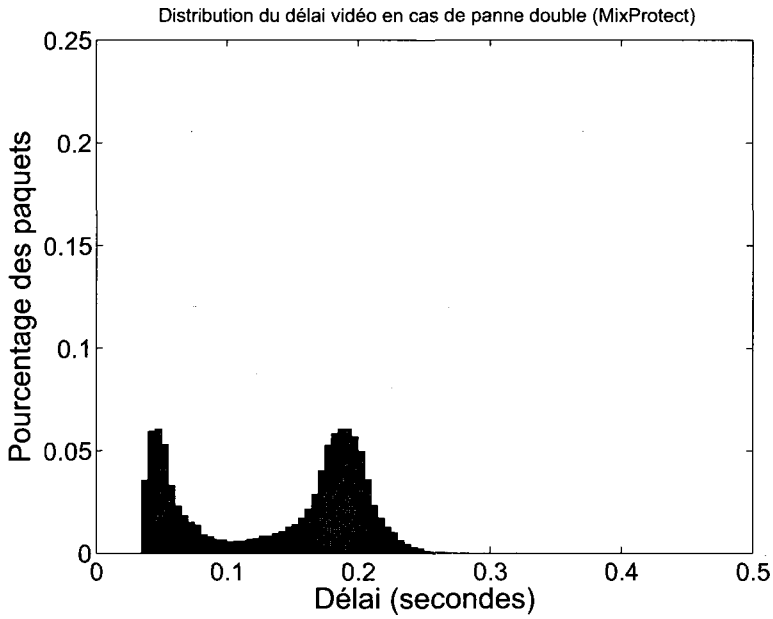


FIG. 3.29 FDP du délai avec DS-DP-DP

Les résultats pour les combinaisons DP-DS-DP et DS-DP-DP sont montrés dans la figure 3.28 et 3.29 respectivement. Nous pouvons voir que l'utilisation de DiffProtect sur le dernier lien du réseau limite le délai à des valeurs inférieures à 300 ms. Des résultats assez similaires sont observés dans la figure 3.30 pour le cas DS-DS-DP où nous observons toujours deux sommets, des valeurs de délai limitées, mais pas à 100%. Ceci implique que l'utilisation seule de DiffProtect au point de sortie du réseau ne peut garantir des bornes sur le délai. Il faut en plus limiter le nombre de liens protégés par DiffServ*, puisque son utilisation croissante offre de moins en moins de garanties sur le délai.

Finalement, la figure 3.31 montre la performance dans le cas du réseau tout-DiffServ*. Près de 50% des paquets ont des délais de moins de 100 ms. L'autre moitié est sujette à des délais très supérieurs et parfois plus grands que 500 ms. Un réseau tout-DiffServ* garantit une performance moyenne meilleure qu'un réseau avec au moins un DiffProtect puisque dans le cas de DiffServ*, un pourcentage plus grand de paquets ont des délais

plus petits.

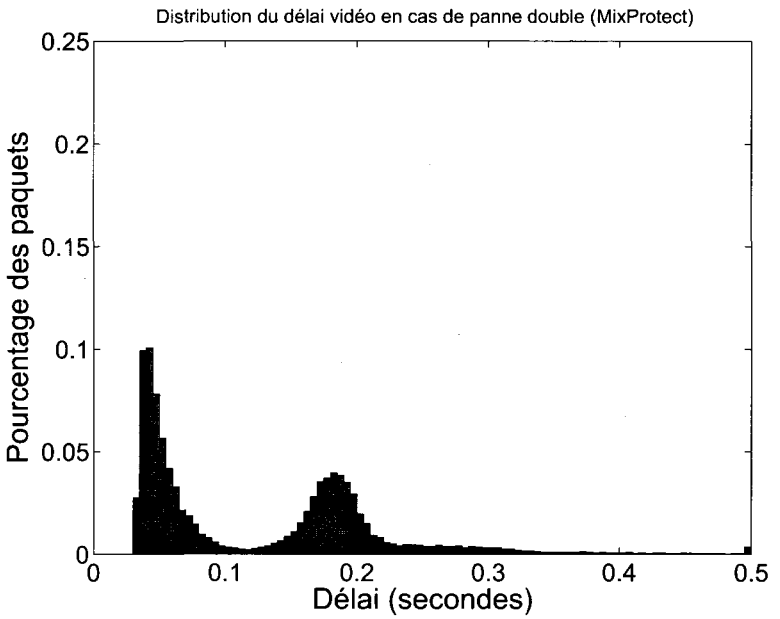


FIG. 3.30 FDP du délai avec DS-DS-DP

Les figures 3.32 et 3.33 montrent les distributions cumulatives du délai du trafic vidéo pour toutes les combinaison de protection en cas de pannes doubles. Nous pouvons voir des deux figures que :

- pour les combinaisons de protection qui se terminent par DiffProtect :
  - le point limite $P = 1$ est atteint plus rapidement,
  - les courbes croissent relativement rapidement entre les points d'abscisses 100 ms et 200 ms ;
- pour les combinaisons qui se terminent par DiffServ* :
  - la marque $P = 1$ est atteinte seulement pour des grandes valeurs de délai,
  - les courbes montrent une augmentation beaucoup plus graduelle.

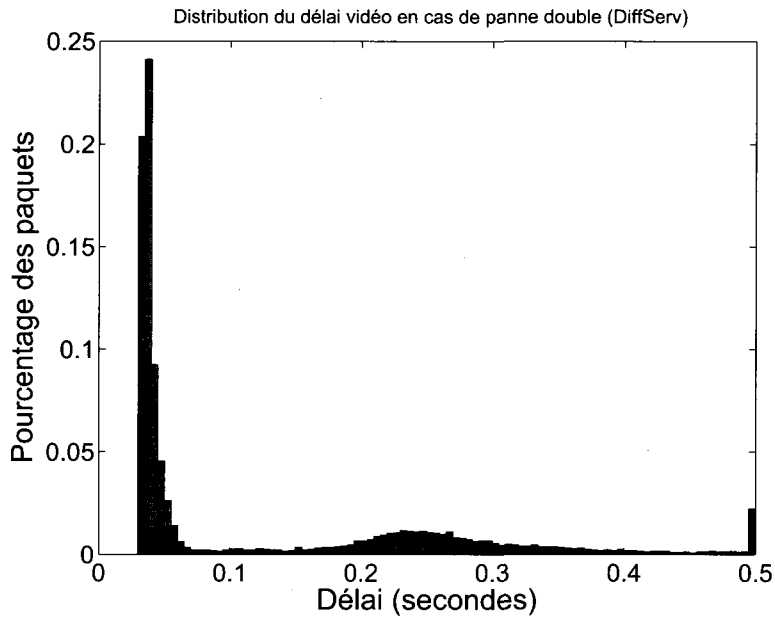


FIG. 3.31 FDP du délai avec DS-DS-DS

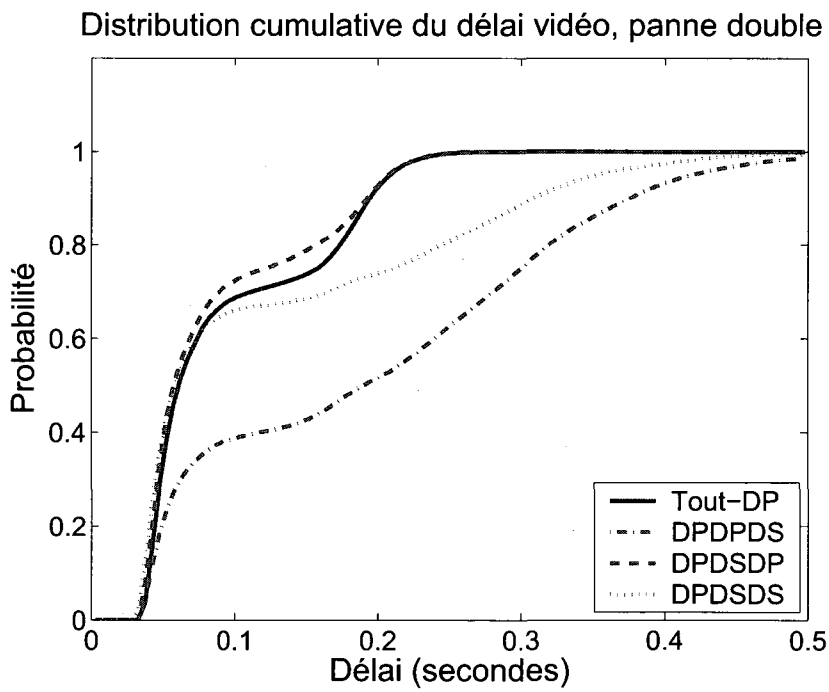


FIG. 3.32 FDC du délai pour combinaisons commençant par DiffProtect

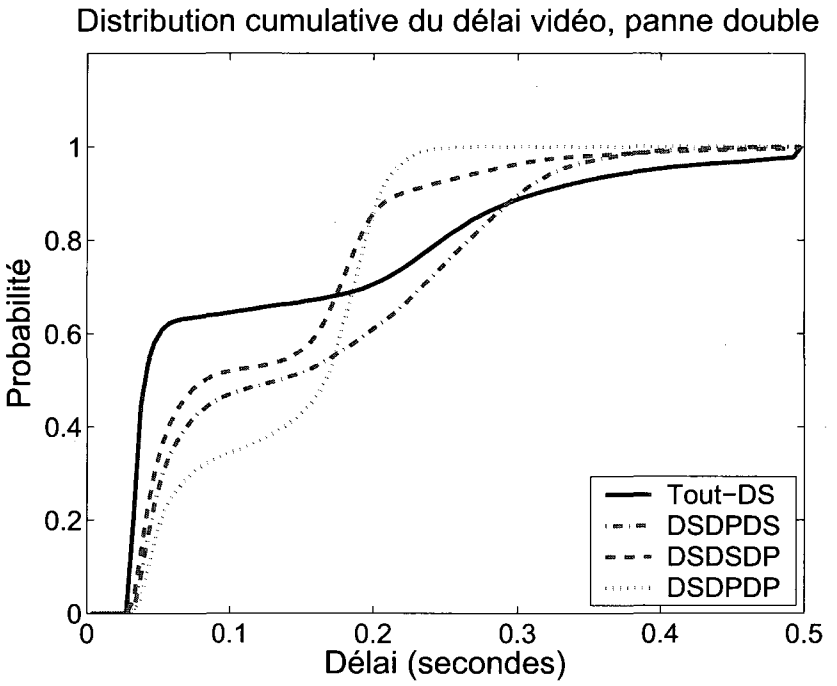


FIG. 3.33 FDC du délai pour combinaisons commençant par DiffServ*

3.3.3.3 Résumé

Les résultats des figures 3.21–3.23 montrent qu'une protection essentiellement basée sur DiffServ* est idéale pour garantir une meilleure performance globale en cas de pannes. Les conclusions principales de notre analyse :

- la protection offerte au trafic EF est relativement invariable quelle que soit la nature de la protection utilisée ;
- quand DiffServ* devient prédominant dans le réseau :
  - nous observons aussi une amélioration systématique de pratiquement toutes les mesures de performance du trafic AF,
  - le taux de perte du trafic BE est à la baisse,
  - ceci est à l'encontre du délai et de la gigue de ce trafic qui se détériore.

Cette pénalité de performance peut être acceptable étant donné la nature du trafic BE qui n'a pas besoin d'une QdS garantie. Si notre objectif est de maximiser la performance

moyenne du réseau, alors DiffServ* est la méthode de choix. Si ce n'est pas le cas, il faut alors considérer des situations particulières de performance, de trafic et de pannes comme dans l'exemple de la section 3.3.3. Nous pouvons avoir, à certains endroits du réseau, que la probabilité des pannes doubles est jugée inacceptable et qu'il faut absolument limiter le délai du trafic AF. Il serait alors conseillé d'utiliser une combinaison MixProtect, tel DP-DS-DP et DS-DP-DP qui selon nos résultats aboutissent à une meilleure performance. Nous pouvons généraliser en suggérant deux directives dans le choix d'une combinaison MixProtect pour un flot ou un réseau. Il faut que :

- la dernière partie d'un chemin utilisé par un flot AF vidéo particulier soit protégée par DiffProtect ;
- le nombre de liens protégés par DiffServ* ne dépasse pas le nombre de ceux protégés par DiffProtect.

Ces conditions doivent être appliquées avec prudence puisque, dans un grand réseau qui est utilisé par plus d'un flot, il est possible d'avoir un lien protégé par DiffProtect qui soit, par exemple, le dernier d'un chemin et le premier lien d'un autre. Ce conflit fera l'objet d'un modèle d'optimisation détaillé dans le chapitre 5.

3.4 Simulations de grands réseaux maillés

Le réseau de la figure 3.34 est simulé pour montrer que la méthode de protection MixProtect est extensible et permet de protéger le trafic de façon adéquate pour des topologies plus complexes utilisées par plus d'un flot. Le réseau comprend trois flots A, B et C qui se croisent. Les performances moyennes d'une protection toute-DiffServ*, toute-DiffProtect et celle de plusieurs combinaisons MixProtect ont été évaluées.

Les modèles DiffServ* et DiffProtect utilisés dans l'étude ci-contre sont identiques à ceux utilisés dans les sections précédentes. Dans le cas de DiffServ*, chaque lien IP est un groupement de chemins optiques, aucune protection n'est disponible au niveau physique

et toute panne de chemin optique cause une réduction au niveau de la capacité du lien logique correspondant. Dans le cas de DiffProtect, trois chemins optiques sont utilisés mais ceux-ci sont munis de chemins de protection qui sont disjoints des chemins optiques primaires.

Pour cette étude, nous simulons la topologie de la figure 3.34. Ce réseau possède les caractéristiques suivantes :

- topologie en maille à six noeuds et sept liens logiques ;
- tous les liens logiques sont des groupements de trois chemins optiques ;
- les chemins optiques d'un lien sont disjoints entre eux et de ceux de tout autre lien logique ;
- trois flots A, B et C croisés et routés sur trois chemins logiques différents.

Dans le cas du réseau de la figure 3.34, aucun multiplexage n'a lieu et tous les canaux optiques sont mis en place sur des chemins physiques différents. Dans ce cas, la coupure d'une fibre optique produit la panne d'un seul chemin optique et affecte un seul des sept liens logiques du réseau IP. Cette configuration n'est pas très réaliste puisque dans un réseau IP/WDM réel, les canaux optiques de deux liens logiques différents peuvent partager une ou plusieurs fibres optiques. Dans ces conditions, la coupure d'une fibre entraîne la panne d'un ou plusieurs chemins optiques de deux ou plusieurs liens logiques simultanément. Dans ce cas, les pannes des liens logiques deviennent dépendantes entre elles, dépendantes de l'assignation physique des canaux optiques et donc de la topologie physique utilisée. Si nous voulions considérer tous ces détails, nos simulations seraient non seulement plus complexes, mais aussi dépendantes de l'assignation optique des connexions et de la topologie physique utilisée.

Notre intérêt principal est d'étudier *l'effet* des pannes optiques sur la couche logique sans contraintes sur la disposition des connexions optiques et de la topologie physique. Dans cette optique, nous considérons que les pannes des liens logiques ont lieu sur des chemins

physiques séparés et sont donc indépendantes. Cette pratique permet d'avoir des pannes de tout type qui peuvent affecter toute combinaison de liens logiques simultanément ou séparément. Notre étude devient alors indépendante d'une topologie physique fixe et donc permet d'obtenir des résultats applicables dans tout type de réseau.

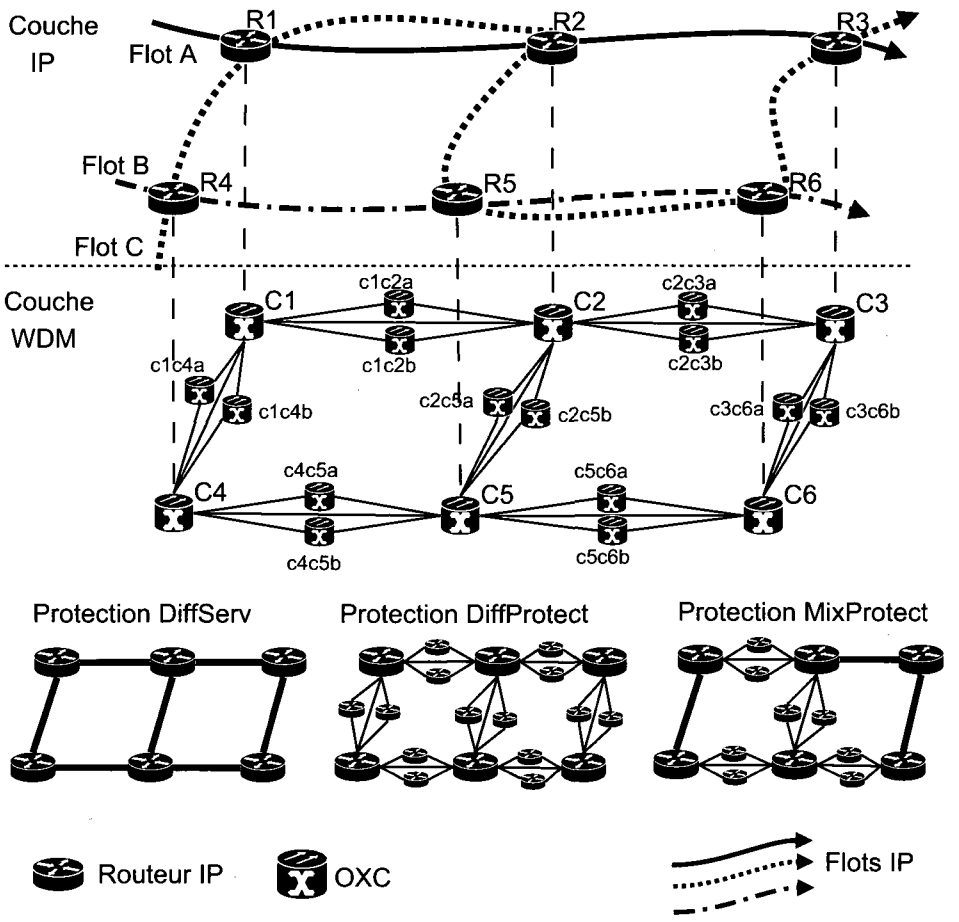


FIG. 3.34 Simulation d'un réseau en maille à noeuds.

Dans nos simulations :

- les flots A, B et C ont les mêmes caractéristiques de trafic et débits que ceux des sections précédentes ;
- le flot A est routé sur le chemin $(1, 2, 3)$;
- le flot B utilise le chemin $(1, 4, 5, 2, 3, 6)$;
- le flot C est mis sur le chemin $(4, 5, 6)$;

- pour assurer un dimensionnement adéquat du réseau :
  - les liens $(1,2)$, $(1,4)$, $(2,5)$, $(3,6)$ et $(5,6)$ sont utilisés par un seul flot et ont un débit de 15 Mbps,
  - les liens $(2,3)$ et $(3,4)$ sont utilisés par 2 flots, leur capacité est de 30 Mbps chacun.

L'objectif principal de cette étude et de vérifier si les résultats obtenus précédemment restent valables pour des topologies de réseau plus générales. Nous nous concentrons aussi sur la performance perçue par le flot B puisqu'il utilise un nombre relativement grand de liens et doit partager l'utilisation des ressources de transmission de deux des liens qu'il utilise.

Nous étudions la topologie de la figure 3.34 sous différentes combinaisons de protection MixProtect. Une des combinaisons étudiées est quand tous les liens sont protégés par DiffServ*, une autre quand tous utilisent DiffProtect. En considérant le nombre de liens dans le réseau, le nombre total de combinaisons DiffServ* et DiffProtect possible est de $2^7 - 2 = 126$. Étant trop nombreux à simuler en totalité nous étudions la qualité de la protection des diverses combinaisons MixProtect en fonction du nombre croissant de liens qui utilisent DiffServ*.

Nous considérons en premier un réseau entièrement protégé par DiffProtect, nous choisissons ensuite au hasard, 6 combinaisons de protection dont :

- deux ont 25% des liens protégés par DiffServ* et 75% par DiffProtect ;
- les deux MixProtect suivants sont à 50-50 entre DiffServ* et DiffProtect ;
- les deux derniers ont 75% des liens qui utilisent DiffServ* et le reste DiffProtect.

Finalement, nous avons le cas où le réseau est entièrement protégé par DiffServ*. La table 3.2 montre les différentes combinaisons de protection utilisées telles que perçues par les différents flots. Chacune des huit combinaisons a été simulée à vingt reprises à chaque fois soumise à un scénario de panne différent. Nous calculons par la suite la moyenne, à des intervalles de confiance de 95%, des taux de pertes, délai et gigue de chaque combi-

	Flot A	Flot B	Flot C
0%DS-100%DP	DP-DP	DP-DP-DP-DP-DP	DP-DP
25%DS-75%DP (a)	DP-DS	DP-DP-DP-DS-DS	DP-DP
25%DS-75%DP (b)	DP-DS	DP-DS-DP-DS-DP	DS-DP
50%DS-50%DP (a)	DP-DP	DP-DS-DS-DP-DS	DS-DP
50%DS-50%DP (b)	DP-DS	DS-DS-DP-DS-DS	DS-DP
75%DS-25%DP (a)	DS-DS	DP-DP-DS-DS-DS	DP-DS
75%DS-25%DP (b)	DP-DP	DS-DS-DS-DP-DS	DS-DS
100%DS-0%DP	DS-DS	DS-DS-DS-DS-DS	DS-DS

TAB. 3.2 Protection mixte des flots

naison de protection. Les résultats sont présentés dans les figures 3.35, 3.36 et 3.37 pour le flot B et dans les figures 3.38, 3.39 et 3.40 pour le réseau complet.

Pour plus de visibilité dans les figures 3.35 et 3.38, le taux de perte des paquets EF et ceux des flots AF et BE ont été tracés sur deux échelles différentes. L'échelle de droite est utilisée pour montrer avec plus de détails les effets de la variation de la combinaison de protection sur les taux de pertes du trafic EF. À gauche nous avons l'échelle des pertes AF et BE.

Les taux de pertes de paquets du flot B sont montrés dans la figure 3.35 :

Le passage d'un réseau tout-DiffProtect à un réseau tout-DiffServ* influence différemment chaque classe de trafic du flot B. Quand plus de liens sont protégés par DiffServ*, nous avons :

- une faible augmentation de taux de perte des paquets de voix EF ;
- un inconvénient mineur vu que nous observons en contre-partie que :
  - moins de paquets AF sont perdus,
  - le taux de perte BE diminue d'approximativement 50%.

Le délai moyen des différentes classes de trafic du flot B est montré à la figure 3.36. Nous pouvons voir que :

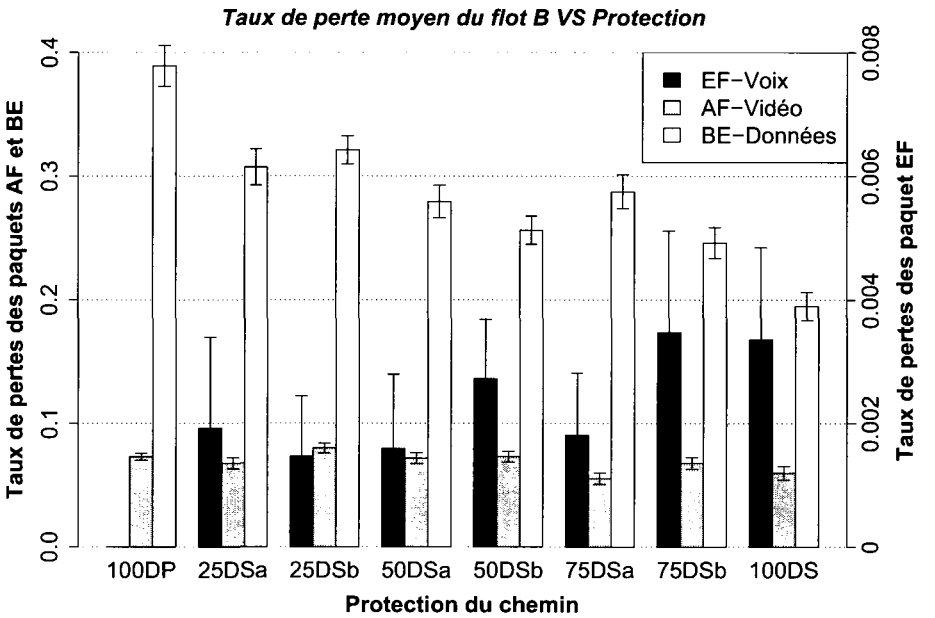


FIG. 3.35 Taux de pertes moyen, flot B

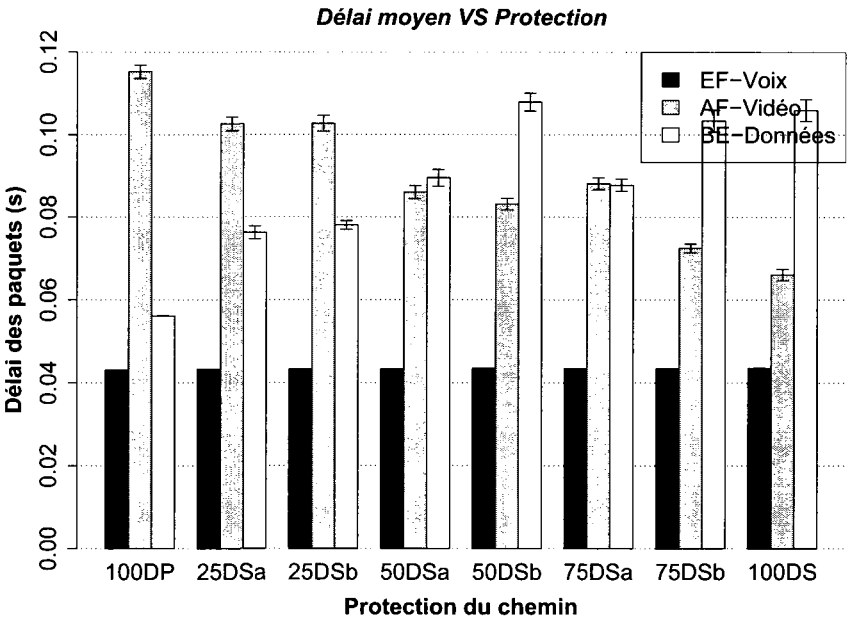


FIG. 3.36 Délai moyenne, flot B

- Le délai des paquets de voix est constant quelle que soit la combinaison de protection utilisée.
- Celui du trafic AF diminue quand DiffServ* devient prédominant dans le réseau.
- Le délai du trafic BE augmente quand le ratio DiffServ*/DiffProtect augmente.

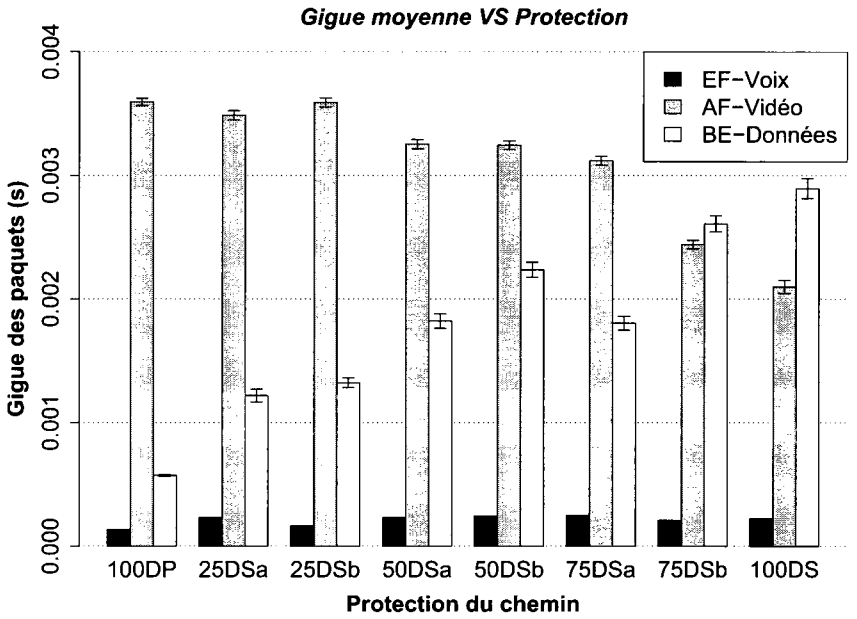


FIG. 3.37 Gigue moyenne, flot B

La gigue du trafic de voix, vidéo et données du flot B est montrée à la figure 3.37. Quand plus de liens sont protégés par DiffServ*, nous observons que :

- la gigue du trafic EF n'est pas affecté par le changement de protection ;
- la gigue de la classe AF diminue ;
- celle du trafic de donnée augmente.

Les conclusions de l'analyse ci-dessus et celles de l'étude du réseau linéaire à quatre noeuds sont très similaires. Ceci nous permet de confirmer que les résultats restent valides pour des chemins dont la longueur dépasse quatre noeuds et même en présence de plus d'un flot qui l'utilise en totalité ou en partie.

Les figures 3.38, 3.39 et 3.40 montrent respectivement le taux de perte moyen, le délai

moyen et la gigue moyenne pour le réseau entier. Ces résultats sont obtenus en calculant la moyenne des taux de perte, délais et gigues des flots A, B et C. Ces graphiques permettent de tirer les mêmes conclusions que nous avons obtenues précédemment. L'utilisation croissante de DiffServ* comme mécanisme de protection dans un réseau améliore les valeurs de la qualité de service moyenne telle que perçue par les flots.

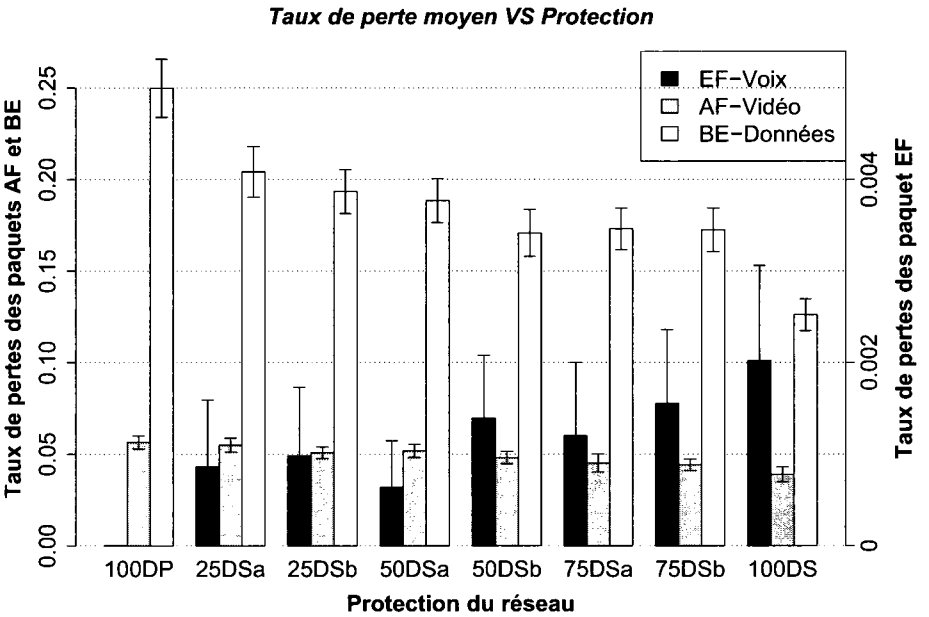


FIG. 3.38 Taux de perte moyen, réseau

La figure 3.38 montre un taux de perte décroissant pour les flots AF et BE et croissant pour le trafic EF.

Délai et gigue sont visualisés dans les figures 3.39 et 3.40 respectivement.

- pour le délai :
  - le délai moyen du trafic de voix est constant quelle que soit la combinaison de protection utilisée,
  - le délai des flots vidéos décroit de près d'un tiers alors que celui des paquets de données augmente ;

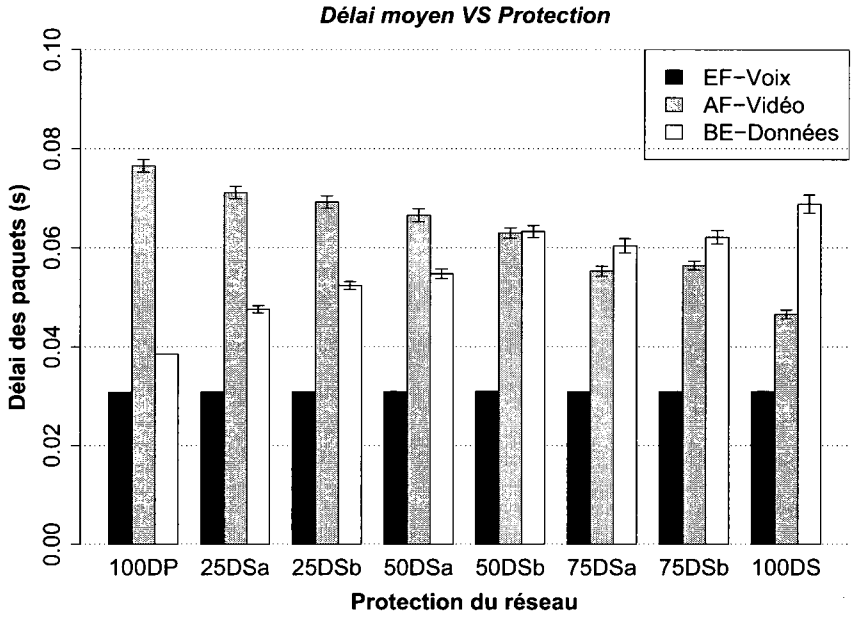


FIG. 3.39 Délai moyen, réseau

- pour la gigue :
  - la gigue des flots de voix augment très légèrement quand DiffServ* est utilisé davantage ;
  - pour le trafic vidéo, la gigue :
    - reste constante tant que moins de la moitié des liens sont protégés par DiffServ*,
    - diminue de près d'un tiers quand plus de 75% des liens utilisent DiffServ* ;
  - la gigue des paquets BE double quand on compare les protections tout-DiffProtect et tout-DiffServ*.

Cette section confirme nos observations de performance précédentes pour des réseaux à flot unique :

- le modèle de protection de trafic DiffServ* est capable de fournir une meilleure fiabilité que DiffProtect ;
- pour une réduction très faible dans la performance des flots EF :
  - DiffServ* est meilleur dans la protection des flots AF et BE contre les dégradations

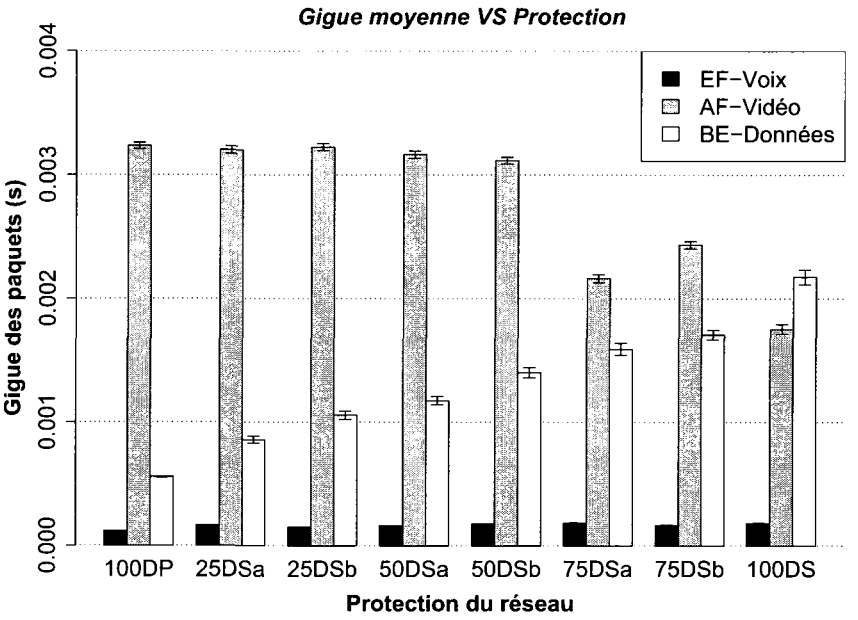


FIG. 3.40 Gigue moyenne, réseau

majeures de performance en cas de pannes.

Il est important de noter qu'avec DiffServ* la protection du trafic prioritaire en cas de pannes se fait aux dépends du trafic BE de plus basse priorité. Nous avons remarqué qu'il est possible de diminuer l'impact de la panne sur cette catégorie de trafic en utilisant ce que nous appelons le routage par déflexion ; nous présentons une description de cette solution dans l'annexe III.

Nous montrerons dans le chapitre suivant que les bénéfices de DiffServ* se comptent autant en gains en protection et performance, mais aussi dans des économies dans la quantité de ressources nécessaires au déploiement d'un réseau de prochaine génération multiservice et fiable.

L'approche par simulation permet d'évaluer, pour des réseaux de petites tailles, la combinaison de protection optimale aux différentes priorités de trafic. Une analyse exhaustive par simulation devient impossible quand on traite des grands réseaux. Ceci est dû au fait

que le nombre de combinaison augmente exponentiellement avec le nombre de liens dans le réseau. Le réseau de la figure 3.34 nécessitera la simulation de $2^7 = 128$ combinaisons de protection différentes pour trouver exactement la meilleure. 32768 combinaisons existent pour un réseau contenant 15 liens.

Il est alors primordial de développer un modèle analytique qui optimise le déploiement DiffServ*/DiffProtect de protection différenciée multicouche pour un réseau de toute taille. Cette combinaison maximise la qualité de service offerte aux trafics de hautes priorités en cas de pannes et permet de minimiser considérablement le coût associé à la redondance et le surdimensionnement des ressources physiques. Cette étude fait l'objet du chapitre 6.

CHAPITRE 4

ANALYSE DE FIABILITÉ, DE COÛTS ET ÉTUDE DE CAS

Nous avons évalué au cours du chapitre précédent, la performance de DiffServ* du point de vue *du trafic*. Pour cela, nous avons considéré la qualité de service et le niveau de protection offerts à chaque classe de trafic comme métriques et nous avons conclu que DiffServ* est assurément capable de protéger le trafic prioritaire en cas de pannes physiques dans le réseau. Nous avons aussi établi que grâce au déploiement *lien-par-lien* de DiffServ*, la topologie logique devient pratiquement immunisée contre les pannes de liens. Il faudrait une multitude de pannes simultanées de composantes optiques pour causer la panne totale d'un lien logique. Étant donné que nous voulons porter une attention particulière à ce supplément considérable en fiabilité, l'objectif principal de ce chapitre est de montrer qu'un déploiement généralisé de DiffServ* sur tous les liens logiques d'un réseau permet non seulement d'accroître leur robustesse face aux pannes mais aussi de réaliser des économies importantes en ressources de transmission. Nous démontrons ce point de vue dans les section 4.1 et 4.2 dans lesquelles la fiabilité et le coût de déploiement d'un réseau logique protégé par DiffServ* sont évalués.

La section 4.1 compare la fiabilité de deux réseaux IP/WDM démunis de tout mécanisme de protection optique où l'un applique la technique standard de routage de connexions optiques et l'autre celle de DiffServ*. Quant à la section 4.2, celle-ci montre la quantité de ressources de transmission nécessaire au déploiement des modèles DiffServ* et DiffProtect dans un réseau IP/WDM. Elle montre que, même en terme d'utilisation des ressources de transmissions, les modèles DiffServ* et DiffProtect sont avantageux par rapport à une méthode de protection plus traditionnelle. Par la suite, une *étude de cas* est réalisée à la section 4.3 et a comme objectif d'étudier la position des nouveaux modèles

de protection différenciée DiffServ* et DiffProtect par rapport aux propositions et architectures récentes pour les réseaux de prochaine génération. Plus particulièrement, cette section décrit le fonctionnement de MPLS DiffServ-TE et montre la compatibilité entre cette architecture et les modèles de protection DiffServ* et DiffProtect. Nous présentons par la suite une étude qui montre l'avantage en fiabilité qu'a l'intégration de DiffServ* dans l'environnement MPLS-DS-TE.

4.1 Fiabilité des réseaux logiques protégés par DiffServ*

La grande différence entre un réseau IP/WDM standard et celui avec DiffServ* est le routage physique des connexions optiques d'un groupement logique. Dans le cas des réseaux IP/WDM réguliers, les canaux optiques qui forment chaque groupement de liens sont mis en place sur le chemin physique le plus court qui sépare les extrémités du lien logique en question. Ceci est illustré à la figure 4.1 dans laquelle les composants du lien logique $(R1, R2)$ sont mis en place sur le lien physique sous-jacent $\{C1, C2\}$. Il en est de même pour les liens $(R1, R3)$, $(R1, R4)$, $(R3, R2)$ et $(R4, R2)$ qui constituent la topologie physique.

Avec DiffServ*, les canaux optiques d'un lien logique doivent être séparés et mis sur des chemins disjoints physiquement. Ceci est nécessaire pour préserver leur indépendance en cas de pannes physiques. Un exemple du routage DiffServ* est illustré à la figure 4.2. Dans ce cas, un chemin optique du lien $(R1, R2)$ est mis en place sur le lien physique direct $\{C1, C2\}$, un deuxième sur $\{C1, C3, C2\}$ et un troisième sur $\{C1, C4, C2\}$. Le même principe s'applique pour les autres liens du réseau logique.

Les couches logiques des figures 4.1 et 4.2 sont topologiquement identiques mais diffèrent seulement dans la façon utilisée pour leur mise en place. Il est nécessaire de mentionner aussi que les deux réseaux n'emploient aucun mécanisme de protection physique. Nous

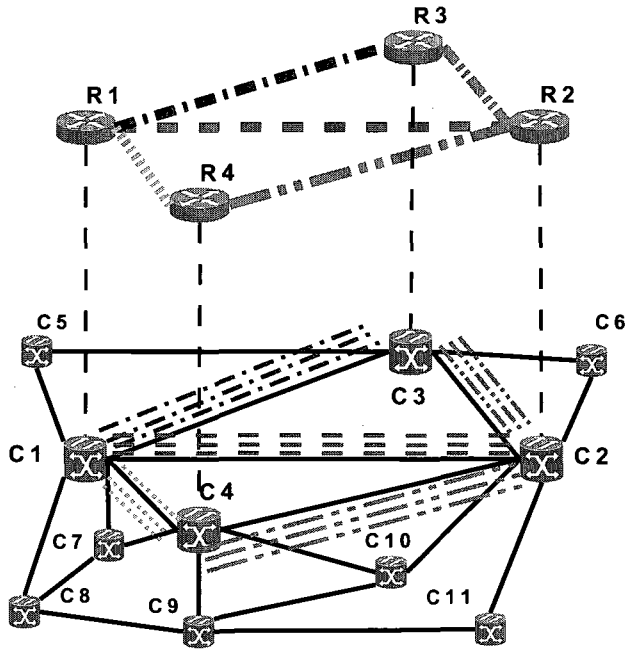


FIG. 4.1 Routage et assignation de longueurs d'onde normal

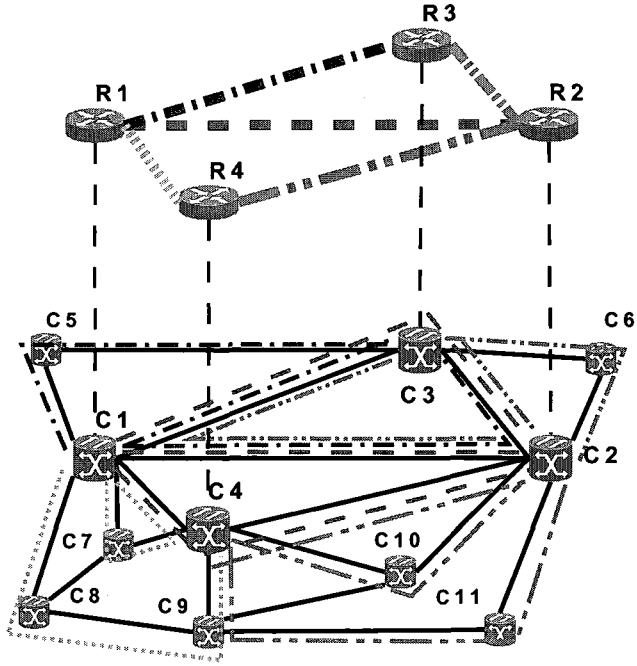


FIG. 4.2 Routage et assignation de longueurs d'onde DiffServ*

pouvons alors calculer les probabilités de pannes des liens logiques en fonction de celles des différents liens physiques du réseau.

Si $P[C_{ij}]$ est la probabilité qu'un lien physique $[i, j]$ soit en panne alors la probabilité qu'un chemin optique C_o soit en panne se calcule à l'aide de la formule :

$$P[C_o] = 1 - \left(\prod_{(i,j) \in C_o} (1 - P[C_{ij}]) \right) \tag{4.1}$$

Nous savons qu'un lien logique ne tombe en panne que si tous ses canaux optiques sont en panne. Dans le cas normal, la probabilité de panne d'un lien logique est égale à la probabilité de panne du seul chemin optique utilisé pour le routage de ses connexions. Avec DiffServ*, la probabilité de panne d'un lien logique est égale au produit des probabilités de panne de tous les chemins optiques sous-jacents. Le tableau 4.1 montre les résultats de ces calculs pour une valeur $P[C_{ij}]$ $\forall i, j$. Dans la colonne de gauche nous voyons les probabilités de panne des différents liens de la topologie logique dans le cas normal sans protection, à droite se trouvent les probabilités de panne, nettement inférieures, des liens DiffServ*. À titre indicatif, la colonne du milieu montre la probabilité de panne des liens logiques dans le cas où les canaux optiques de chacun sont munis de canaux de protection qui leur sont disjoints ; la probabilité de panne du lien logique est dans ce cas égale au produit des probabilités de pannes du chemin optique principal et celui utilisé pour la protection.

Il devient alors évident qu'une deuxième conséquence très importante du déploiement généralisé de DiffServ* sur tous les liens d'un réseau logique est une augmentation considérablement de sa fiabilité et sa robustesse face aux pannes physiques. La coupure d'une fibre optique unique ne peut dorénavant causer la panne complète d'un ou plusieurs liens logiques mais seulement une diminution de son ou leur débit. Nous passons alors d'une situation de *tout ou rien* où les liens logiques peuvent être soit fonctionnels, soit en panne

Lien logique	Probabilités de panne		
	Cas normal		Cas DiffServ*
	Sans protection	Avec Protection	
$(R1, R2)$	0.01	1.99e-04	3.96e-06
$(R1, R3)$	0.01	1.99e-04	3.96e-06
$(R1, R4)$	0.01	1.99e-04	5.96e-06
$(R3, R2)$	0.01	1.99e-04	3.96e-06
$(R4, R2)$	0.01	1.99e-04	5.96e-06

TAB. 4.1 Fiabilité des liens logiques

complète à une situation ou plusieurs échelons de pannes sont possibles. La diminution du débit d'un lien logique dépend du nombre de pannes simultanées au niveau physique et plus ce nombre est élevé, plus sa probabilité est petite.

Une deuxième différence importante entre le cas régulier et celui avec DiffServ* est que la connectivité entre les différents noeuds de la topologie logique est maintenue même en situation de pannes physiques multiples. Ceci est d'une grande importance puisqu'il est possible, à l'aide de DiffServ* seul et sans recours à aucun mécanisme de protection physique, d'augmenter la fiabilité de la couche logique. L'alternative au déploiement de DiffServ* est l'utilisation de mécanismes physiques de protection, cette protection peut être différenciée comme c'est le cas de DiffProtect ou non dans le cas régulier. Ces mécanismes aideront certainement à l'accroissement de la fiabilité de la topologie logique mais comme nous le montrerons dans la prochaine section, DiffServ* demeure économiquement meilleur. Il permet d'offrir un niveau de protection et de fiabilité similaire et parfois meilleur, tout en consommant moins de ressources physiques.

4.2 DiffServ*, DiffProtect et ressources optiques

Cette section compare la quantité de ressources optiques nécessaires au déploiement des deux modèles de protection DiffServ* et DiffProtect dans un réseau IP/WDM à celle de

la technique de protection régulière ou traditionnelle. Nous la définissons comme étant le nombre de longueurs d'onde qu'il faut réserver sur chaque lien physique afin de garantir une capacité de transmission et de protection suffisante à la demande de trafic IP.

4.2.1 Topologie étudiée

Le déploiement des modèles de protection DiffServ* et DiffProtect se fait nécessairement entre deux routeurs IP adjacents donc reliés par un lien IP de capacité supposée connue. Chacun de ces routeurs est relié à un commutateur optique. Les modèles DiffServ* et Diff-Protect nécessitent trois chemins physiquement disjoints entre ces commutateurs. Le degré de chaque commutateur optique doit être d'au moins trois pour satisfaire la contrainte topologique des deux modèles.

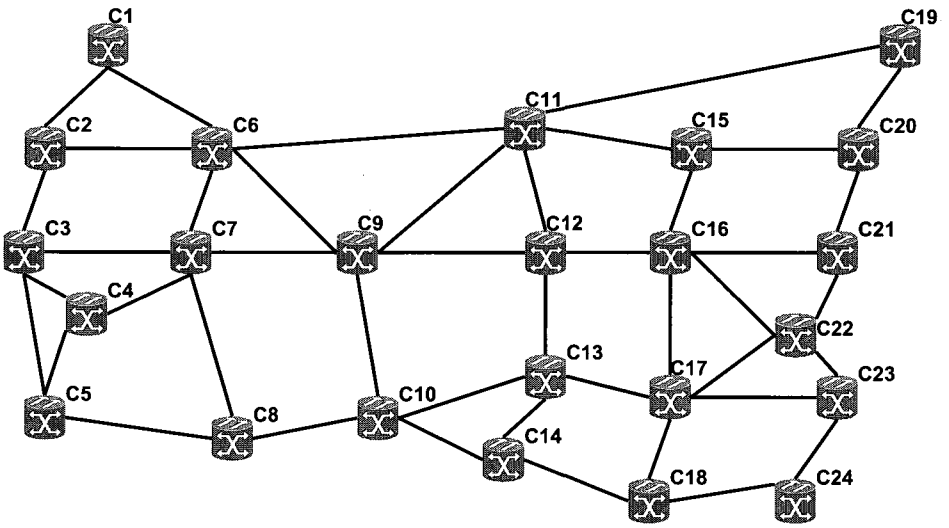


FIG. 4.3 Réseau Optique

La topologie optique considérée pour cette étude est présentée à la figure 4.3. Le degré moyen par commutateur est de 3.5833. Ceci rend la topologie physique suffisamment connexe pour accueillir le déploiement des modèles DiffServ* et DiffProtect.

La figure 4.4 illustre la topologie logique utilisée pour cette étude. Pour simplifier, nous la supposons identique à la topologie physique donc il n'existera un lien logique entre R_i et R_j au niveau IP que s'il existe un lien physique entre C_i et C_j. Comme il est possible de constater, nous avons dans la majorité des cas trois chemins physiques disjoints de disponibles entre chaque paire de routeurs R_i et R_j adjacents.

4.2.2 Demande de trafic IP et capacité de transmission optique

Nous considérons pour l'instant que le dimensionnement de la couche IP est déjà accompli. Nous connaissons la capacité et la quantité de trafic EF, AF et BE de chaque lien logique. Nous considérons que la demande de chaque type de trafic entre deux routeurs adjacents ne requiert pas plus que la capacité d'un canal optique.

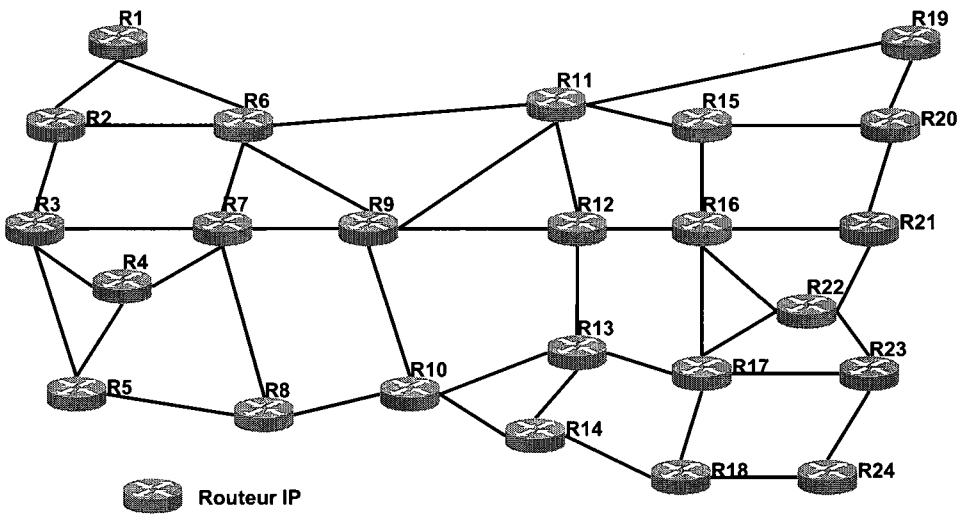


FIG. 4.4 Réseau Logique (IP)

La capacité de chaque lien IP de la figure 4.4 est égale à la somme des capacités des trois canaux optiques qui relient physiquement les deux routeurs. La question est de déterminer comment et où établir ces canaux optiques au niveau physique. Le cas normal sera de réserver ces canaux sur le plus court chemin reliant les routeurs.

Ainsi, pour la topologie IP/WDM des figures 4.3 et 4.4, s'il existe un lien IP entre les routeurs R_i et R_j, trois canaux optiques sont réservés sur le lien physique $[Ci, Cj]$ sous-jacents car dans le cas de ce réseau, $[Ci, Cj]$ est le plus court chemin (PCC) entre R_i et R_j. Nous calculons alors qu'il faut 129 longueurs d'onde sur 43 fibres optiques. Cette demande de trafic est transmise au niveau optique sans aucune protection. Toute coupure de fibre $[Ci, Cj]$ entraîne la panne du lien logique (Ri, Rj) et tout trafic entre R_i et R_j sera perdu s'il n'est pas rerouté.

Il faut déployer plusieurs canaux de protection supplémentaires si nous voulons augmenter la fiabilité de la couche IP. Si la demande de trafic entre R_i et R_j est acheminée sur le lien $[Ci, Cj]$, les canaux de protection peuvent être mis en place sur le deuxième plus court chemin physique reliant C_i et C_j. Cette protection, dite *traditionnelle*, peut être totale. Dans ce cas, trois canaux supplémentaires sont nécessaires pour protéger les trois canaux principaux. La protection traditionnelle peut être partielle si elle prévoit seulement deux canaux de protection pour les trois canaux principaux et pour une protection dédiée des flots EF et AF seulement. La figure 4.5-(b) illustre cette technique de protection traditionnelle. Trois canaux optiques sont nécessaires entre $R6$ et $R11$ et ils sont établis sur le lien $[C6, C11]$. Le deuxième plus court chemin entre $C6$ et $C11$ est $[C6, C9, C11]$ et deux canaux sont réservés sur ce chemin. Le même processus est répété pour le lien $(R10, R13)$. Au total, 14 longueurs d'onde supplémentaires sont nécessaires pour déployer le cas de protection traditionnelle et partielle et 18 sont nécessaires si nous décidons de protéger tout le trafic.

4.2.3 Nombre de longueurs d'ondes, DiffServ* et DiffProtect

La figure 4.5-(a) montre le routage des canaux optiques dans le cas de DiffProtect. Les trois plus courts chemins entre $R6$ et $R11$ sont $[C6, C11]$, $[C6, C9, C11]$ et $[C6, C7, C9, C12, C11]$. Dans ce cas, nous protégeons le canal optique EF à l'aide d'un

autre canal, établi sur le deuxième plus court chemin entre $R6$ et $R11$ soit sur $[C6, C9, C11]$. Le trafic de AF est protégé à l'aide d'un canal de protection partagée établi sur le troisième PCC entre $R6$ et $R11$, soit sur $[C6, C7, C9, C12, C11]$. La même chose est répétée pour le lien IP $(R10, R13)$. Le trafic AF entre $R10$ et $R13$ est protégé par le chemin $[C10, C9, C12, C13]$. Ce canal de protection partage le lien $[C9, C12]$ avec celui qui protège le trafic AF entre $R6$ et $R11$. La protection partagée permet une économie de ressources en réservant une seule longueur d'onde de protection sur le lien $[C9, C12]$ au lieu de deux. Cette longueur d'onde protège uniquement le trafic AF entre $R6$ et $R11$ si $[C6, C9, C11]$ tombe en panne. Elle protège uniquement le trafic AF entre $R10$ et $R13$ si $[C10, C14, C13]$ tombe en panne. Seul un de ces flots est protégé si $[C6, C9, C11]$ et $[C10, C14, C13]$ tombent en panne simultanément. La protection partagée exige beaucoup moins de ressources que la protection dédiée et elle permet de réduire de façon importante le taux de blocage des connexions en cas de pannes et offre une garantie de restauration de 100% en cas d'une panne simple dans le réseau. Plusieurs études montrent les bienfaits de la protection partagée (Zhang and Mukherjee, 2004), (Gowda and Sivalingam, 2003) et (Ramamurthy et al., 2003).

Pour ce déploiement particulier, le modèle DiffProtect requiert en tout 23 canaux optiques, un nombre nettement plus élevé que celui du routage traditionnel. Cependant, DiffProtect a l'avantage d'être plus robuste en cas de pannes multiples. Supposons la panne simultanée des fibres $\{C6, C11\}$ et $\{C6, C9\}$ (relativement proches géographiquement). Dans le cas du routage normal, tout le trafic entre $R6$ et $R11$ est perdu alors que DiffProtect sera capable de protéger une partie de ce trafic.

Le déploiement optique du modèle DiffProtect décrit ci-dessus est différent et plus économique que celui proposé dans le cadre de l'étude de performance du chapitre 3. Cette dernière a permis d'évaluer la performance du modèle DiffServ* en la comparant à la forme la plus fiable de DiffProtect qui requiert que les canaux de protection de EF et AF soient physiquement disjoints des canaux principaux. Évidemment, cette dernière op-

tion requiert davantage de ressources de protection. Ayant déjà montré que DiffServ* est meilleur que DiffProtect dans sa forme la plus robuste, notre but dans cette étude est de montrer que DiffServ* est plus avantageux que DiffProtect dans sa forme la plus économique qui est de réutiliser les mêmes chemins optiques principaux pour les canaux de protection.

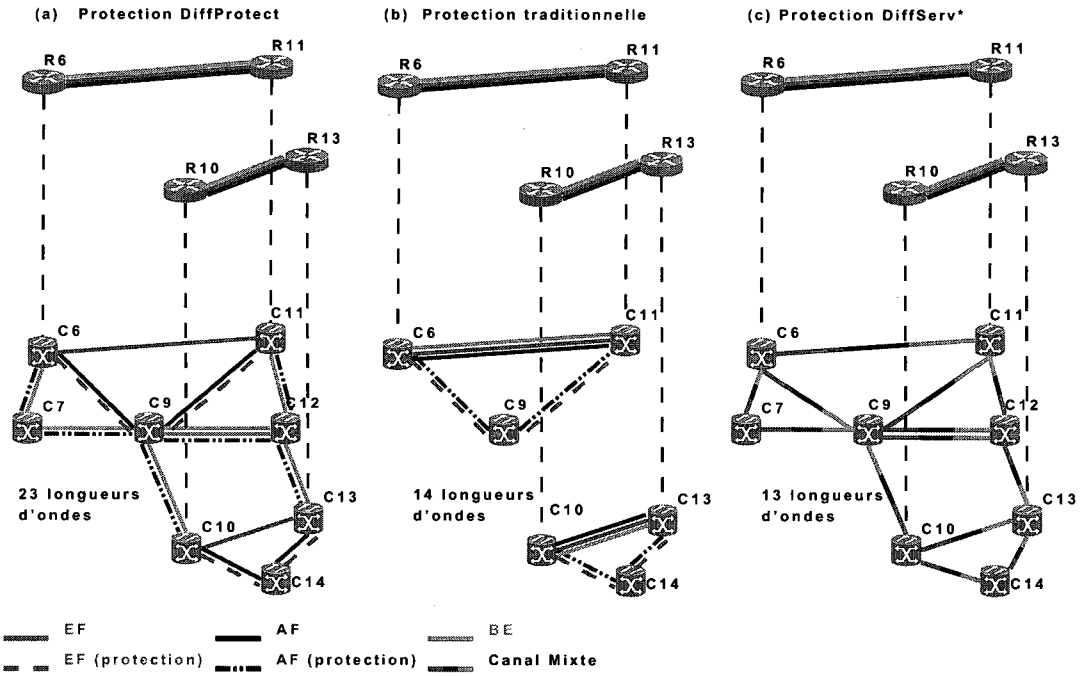


FIG. 4.5 Calcul du nombre de canaux optiques

Finalement la figure 4.5-(c) montre l'allocation électro-optique du trafic dans le cas de DiffServ*. Trois chemins physiques disjoints sont nécessaires dans ce cas aussi. Ces canaux transportent un trafic mixte et la proportion de chaque type de trafic dans un même canal est décidée par le serveur DiffServ et le module d'allocation électro-optique du noeud IP émetteur.

Au total, treize canaux optiques sont nécessaires pour satisfaire la demande de trafic IP ce qui est inférieur au cas traditionnel. De plus, même en cas de pannes multiples, DiffServ sera capable de maintenir une qualité de service et une protection adéquate aux flots

de hautes priorités puisque la protection DiffServ* est indépendante de la localité de la panne. Les trafics de hautes priorités seront seuls à accéder au ou aux canaux optiques fonctionnels.

Reprenons le cas où les liens physiques $[C6, C11]$ et $[C6, C9]$ tombent en panne simultanément. Tout le trafic entre $R6$ et $R11$ est perdu dans le cas de protection traditionnelle. DiffProtect protègera les flots AF et BE entre ces mêmes routeurs. DiffServ* protègera en priorité le trafic EF en le transmettant sur le chemin fonctionnel qui reste. La capacité du chemin $[C6, C7, C9, C12, C11]$ reste partagée entre les flots EF, AF et BE, il sera possible pour DiffServ* de protéger les flots AF et à la limite BE seulement si la demande de trafic EF est inférieure à la capacité du canal optique fonctionnel.

4.2.4 Nombre de longueurs d'onde et topologie complète

Les résultats de la section 4.2.3 montrent déjà qu'il existe un avantage clair dans l'utilisation du modèle de protection différenciée DiffServ* tant pour la protection du trafic de haute priorité que pour son économie en terme de ressources de transmission.

Le processus de calcul du nombre de longueurs d'onde a été appliqué à toute la topologie IP de la figure 4.4. Cependant, certaines modifications sont nécessaires quand il existe moins de trois chemins disjoints entre une paire de routeurs IP adjacents.

4.2.4.1 Existence de 3 chemins disjoints entre deux routeurs

S'il existe trois chemins physiques disjoints entre chaque paire de routeurs, la même méthode de calcul précédente est appliquée. DiffServ* requiert la réservation de trois canaux optiques sur trois plus courts chemins, DiffProtect requiert la réservation de deux canaux de protection supplémentaires pour les trafics de hautes priorités. La méthode de protec-

tion traditionnelle ne nécessite que deux chemins dans ce cas, un pour les trois canaux principaux et un deuxième pour les canaux de protection.

4.2.4.2 Existence de 2 chemins disjoints entre deux routeurs

Dans le cas de DiffServ*, deux des canaux optiques sont placés sur le plus court chemin qu'on suppose être plus robuste en raison de sa plus courte longueur et le troisième est mis sur le deuxième PCC. Dans le cas de DiffProtect, les canaux optiques principaux seront mis sur le PCC et les canaux de protection dédiée et partagée sur le deuxième PCC. Dans ce cas, le déploiement de DiffProtect est similaire à celui de la technique de protection traditionnelle.

4.2.4.3 Existence d'un seul chemin disjoint entre deux routeurs

S'il n'existe qu'un chemin entre une paire de routeurs, le routage sera le même pour les trois méthodes de protection : toute la demande de protection est mise sur le PCC et il n'existe aucun autre chemin pour réaliser une redondance.

4.2.4.4 Résultats

Si nous considérons que DiffProtect est utilisé partout dans le réseau, 420 longueurs d'onde sont nécessaires. 275 longueurs d'onde canaux principaux, 104 canaux de protection dédiée et 41 de protection partagée. Dans le cas de la protection traditionnelle, deux solutions sont possibles. Si nous décidons de protéger la totalité du trafic, 441 longueurs d'onde sont nécessaires. 129 principaux et 312 longueurs d'onde pour la protection dédiée. Si nous protégeons seulement deux des trois canaux principaux, 337 longueurs d'onde sont nécessaires dont 208 pour la protection. Finalement, 285 longueurs d'onde

	longueurs d'onde fonctionnelles	longueurs d'onde de protection		Total
		Dédiée	Partagée	
DiffServ*	285	0	0	**285**
DiffProtect	275	104	41	**420**
Traditionnelle : Totale (3/3)	129	312	0	**441**
Traditionnelle : Partielle(2/3)	129	208	0	**337**

TAB. 4.2 Utilisation des ressources : tableau récapitulatif

sont nécessaires quand la protection DiffServ* est appliquée à tous les liens du réseau logique. Le tableau 4.2 résume ces résultats.

Il est clairement avantageux de déployer DiffServ* partout à travers un réseau IP/WDM. Il requiert le moins de ressources, il est capable de protéger les trafics prioritaires en cas de pannes et ne nécessite pratiquement aucune redondance au niveau optique. Les modèles de protection traditionnelle et DiffProtect nécessitent la réservation des canaux optiques utilisés seulement pour la protection du trafic en cas de panne. Ceci constitue une dépense parfois considérable en capacité. Un réseau protégé par DiffServ* évite partiellement cet usage excessif des ressources dédiés à la protection. En d'autres termes, considérons un réseau optique qui possède 441 longueurs d'onde. Cette capacité est suffisante pour déployer la méthode de protection traditionnelle totale. 312 de ces longueurs d'onde ne sont utilisés qu'en cas de pannes. DiffServ* requiert 285 longueurs d'onde, $441 - 285 = 156$ longueurs d'onde restent utilisables, pour accommoder toute augmentation ou surcharge de trafic IP.

Nous généralisons notre étude à des réseaux IP/WDM où les topologies logiques et physiques sont générées indépendamment l'une de l'autre. Dans chacun des cas, le nombre de liens physiques est aléatoire mais suffisant pour assurer un minimum de deux chemins disjoints entre toutes paires de noeuds logiques du réseau. Le tableau 4.3 montre le nombre de longueurs d'onde nécessaire aux protections tout-DiffServ*, MixProtect (70% DiffServ*, 30% DiffProtect), tout-DiffProtect, traditionnelle partielle et totale pour des to-

Numbre de Noeuds	10	20	50	100
DiffServ*	308	715	3000	6655
MixProtect	355	815	3511	7652
DiffProtect	431	1000	4160	9299
Traditionnelle : Partielle(2/3)	439	1077	4415	10143
Traditionnelle : Totale (3/3)	546	1332	5430	12420

TAB. 4.3 Utilisation des ressources : tableau récapitulatif

pologies de dix, vingt, cinquante et cent noeuds. Nous pouvons voir que DiffServ* reste la technique la plus économique quelle que soit la grandeur du réseau. La méthode hybride MixProtect et même DiffProtect requièrent dans tous les cas moins de ressources que la protection traditionnelle. Ceci démontre encore l'avantage en fiabilité, en performance et en économie de ressources des méthodes de protection différenciée que nous proposons.

4.3 MPLS-DiffServ TE

Les résultats obtenus au chapitre 3 et aux sections précédentes nous affirment que Diff-Serv* est le mécanisme de protection différenciée favori autant par sa capacité de protéger le trafic en cas de congestion et panne, par prédisposition à augmenter considérablement la fiabilité du réseau logique que par l'économie en ressources de transmissions physiques qu'il introduit. Il existe cependant certains préalables au déploiement des modèles de protection différenciée DiffServ* et DiffProtect :

- les deux modèles reposent sur l'utilisation :
  - de la technique de groupement de liens par séparation,
  - du partage de charge du trafic ;
- le modèle DiffServ* requiert la présence de l'architecture des services différenciés dans la couche logique ;
- le modèle DiffProtect requiert l'utilisation de mécanismes de protection optiques dans la couche physique.

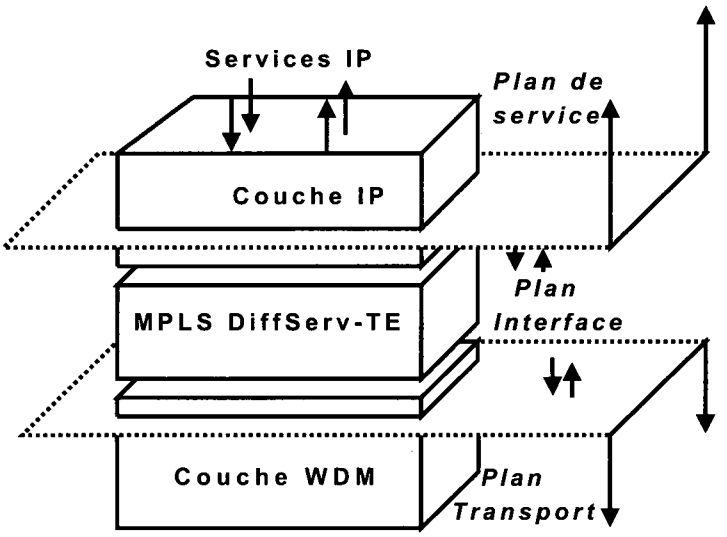


FIG. 4.6 Service, MPLS-DiffServ TE and Transport Planes

Une analyse préliminaire de la proposition *MPLS DiffServ-aware Traffic Engineering (MPLS DiffServ-TE)* pour les réseaux IP/WDM de prochaines générations montre que celle-ci possède tous les éléments de base requis par DiffServ* et au besoin, DiffProtect. En fait, MPLS DiffServ-TE a été développé pour combiner les avantages de MPLS, Diff-Serv et de l'ingénierie de trafic (TE) dans le but de déployer un réseau capable d'offrir une qualité de service stricte à différentes classes de trafic. Comme nous le montrons dans la figure 4.6, MPLS-DS-TE joue le rôle d'interface entre la couche logique de service et la couche physique de transport de l'information. Cette architecture permet entre autres d'optimiser l'allocation de la bande passante aux différentes classes de trafic d'un réseau IP/MPLS tout en leur garantissant les ressources qui leur sont nécessaires pour maintenir leurs exigences minimales de QdS. Après une description détaillée de l'environnement MPLS-DS-TE, nous étudions dans cette section la possibilité de l'utiliser pour une implémentation directe et presque intuitive des deux modèles de protection. L'avantage de cette étude est double, d'un côté nous analysons un environnement qui remplit toutes les exigences de déploiement de DiffServ* et potentiellement DiffProtect et qui bénéficie grandement des ajouts en fiabilité de ces derniers.

4.3.1 Description de MPLS-TE

Dans les réseaux IP traditionnels, l'acheminement des paquets se fait à chaque noeud de façon indépendante. Chaque routeur intermédiaire examine la destination d'un paquet et le transmet sur le plus court chemin disponible ; ce dernier est calculé à l'aide d'un protocole de routage interne tel *Open Shortest Path First (OSPF)*. En général, cette pratique ne tient pas compte de la charge de trafic des liens et résulte en une utilisation sous-optimale de la bande passante disponible du réseau, certains chemins pouvant devenir surchargés alors que d'autres restent sous-utilisés.

Pour éviter les problèmes de surutilisation, MPLS-TE permet de choisir le routage de certains flots de façon explicite, favorisant ainsi explicitement certains chemins, potentiellement sous-optimaux mais qui possèdent les ressources nécessaires, aux chemins les plus courts habituels. Ce routage explicite de l'information diminue la congestion, améliore la performance et assure un meilleur taux d'utilisation de la bande passante du réseau.

Un *Label Switched Path (LSP)* est établi pour chaque flot de données. Chaque LSP possède un LSR source, un LSR destination et une bande passante requise minimale. Le LSP est établi sur un chemin qui possède les ressources nécessaires. La bande passante minimale requise par le LSP est réservée sur chaque lien (*TE Link*) du chemin choisi. MPLS-TE permet de garantir la disponibilité des ressources de transmission pour toute la durée de vie du LSP. MPLS permet en plus d'accroître la fiabilité d'un réseau en offrant des mécanismes additionnels de reroutage rapide de LSP et de protection en cas de pannes.

4.3.2 Rôle de DiffServ

L'ajout de DiffServ rend MPLS-TE conscient de la notion de classe de service (CoS). Il permet la réservation de ressources et la protection du trafic par classe de service et non seulement par LSP. Combinant les fonctionnalités de DiffServ et de TE, MPLS DiffServ-TE assure des garanties de services strictes répondant à des *Service Level Agreements* (SLA) strictes. Des mécanismes de contrôle d'admission de connexion (CAC) et de *Traffic Policing* assurent un respect rigoureux de ces SLA.

4.3.3 Combiner MPLS-TE et DiffServ

L'idée de combiner MPLS et DiffServ a été définie dans plusieurs références notamment (Faucheur and Lai, 2003; Faucheur et al., 2002; Minei, 2004). Un premier défi dans l'intégration des fonctionnalités de DiffServ dans un domaine MPLS est de rendre le DSCP d'un paquet visible dans l'entête MPLS. Dans un réseau DiffServ, le DSCP d'un paquet détermine la classe d'un paquet, EF, AFxy ou BE, donc son *Per Hop Behavior (PHB)*. Le DSCP est généralement encodé sur 6 bits dans l'entête IP d'un paquet et cette entête n'est pas accessible à la couche MPLS. Il est alors nécessaire d'encoder le DSCP au niveau du shim-Header MPLS. Le seul endroit possible est le champ EXP de longueur 3 bits. Un problème se pose sur l'encodage d'une information sur 6 bits dans un espace limité à 3 bits.

Une première solution est de déduire le PHB d'un paquet d'après les bits EXP seulement, ceci donne lieu à des E-LSP. Dans un tel réseau, seulement $2^3 = 8$ classes de service sont possibles. Les paquets d'un même E-LSP peuvent avoir des bits EXP différents, un même E-LSP peut contenir des paquets appartenant à un maximum de 8 classes de service différentes.

Une deuxième solution est celle des L-LSP dans laquelle le PHB d'un paquet est déterminé par l'étiquette (*Label*) d'un LSP et des bits EXP. Par exemple, l'étiquette du LSP peut déterminer la classe EF, AFx ou BE d'un paquet, les bits EXP peuvent déterminer sa préséance de rejet (le y dans AFxy). Dans ce cas, les paquets d'un L-LSP ne peuvent appartenir qu'à une seule classe. Un réseau qui ne nécessite pas plus de 8 classes de services différentes peut utiliser des E-LSP seulement. Un réseau à plus de 8 classes peut combiner les E-LSP et les L-LSP ou utiliser des L-LSP seulement.

4.3.4 Technique de groupement de liens dans un réseau MPLS-TE

La littérature montre que le groupement de liens est très populaire au sein des réseaux IP/MPLS sur WDM. L'application de cette technique dans un réseau MPLS-TE est expliquée en détail dans (Kompella et al., 2005). Pour un réseau MPLS, un groupement de liens relie deux LSR. Ce lien est aussi connu sous le nom d'un *lien TE*. Un lien TE est fonctionnel quand au moins un de ses liens composants est fonctionnel. Un LSP qui traverse un groupement de liens est affecté à un de ses liens composants, la capacité d'un LSP ne peut dépasser celle d'un lien composant et tous les paquets d'un même LSP sont transmis sur le même lien composant. Ceci assure une transmission de bout-en-bout ordonnée des paquets.

Selon (Widjaja and Elwalid, 2003), le groupement de liens est nécessaire parce qu'il permet d'augmenter l'extensibilité du routage quand les LSR sont reliés par plusieurs liens de communications parallèles qui possèdent des attributs similaires. Selon les auteurs, une demande de réservation d'une limite en bande passante B d'un LSP ne peut être acceptée à l'intérieur d'un groupement de lien, que si au moins un lien composant possède une bande passante non réservée et supérieure à B. Les auteurs proposent alors un algorithme, le *Link Bundling with Distributed Traffic Assignement (LB-DA)* qui permet d'établir un LSP sur deux ou plusieurs liens composants si ces derniers possèdent ensemble, la bande

passante nécessaire. Le trafic d'un LSP est ainsi divisé et cette division doit se faire par flot dans le but de respecter l'ordre de transmission et réception des paquets. Dans le cas du LB-DA, la bande passante requise par un LSP est comparée à celle non utilisée du groupement de liens entier et non à celles de ses composantes unitaires. Le LB-DA améliore la performance d'un réseau MPLS en réduisant le taux de blocage de LSP.

Plusieurs références tel (Papadimitriou et al., 2003; Feng et al., 2003), démontrent l'utilité et détaillent le déploiement du groupement de liens au sein des réseaux MPLS/optique. D'ailleurs (Feng et al., 2003) montre qu'il est possible d'avoir des *Component Links* établis sur des chemins physiques séparés. Ce résultat est essentiel au déploiement des modèles DiffServ* et DiffProtect qui requièrent un *Link Bundling* d'un minimum de trois canaux optiques établis sur trois chemins physiquement disjoints.

4.3.5 MPLS DiffServ-TE, DiffServ* et DiffProtect

Nous considérons une topologie MPLS DiffServ-TE dans laquelle la capacité de chaque lien entre deux LSR adjacents est supposée connue. Étant donnée une matrice de trafic, MPLS DiffServ-TE permet de maximiser l'utilisation des ressources de transmission en optimisant la répartition de la demande de trafic sur toute la topologie logique pour fournir des garanties strictes en QdS à toutes les classes de service. MPLS-TE se charge de l'admission des LSP et de la réservation de la bande passante qu'ils requièrent. DiffServ surveille le débit de trafic sur chaque lien et protège les flots de hautes priorités contre toute congestion éventuelle. Le résultat de toutes ces opérations est une répartition du trafic qui respecte les exigences des classes EF, AF et BE sur chaque lien logique du réseau. Dans le cas d'une panne de lien, MPLS-TE se charge de rerouter les LSP affectés par la panne et les protocoles de réservation de ressources, de contrôle d'admission et DiffServ s'occupent de gérer adéquatement les ressources restantes et fonctionnelles du réseau pour assurer une meilleure survie des flots de hautes priorités.

Le processus MPLS DiffServ-TE dépend intrinsèquement de la topologie MPLS et plus spécifiquement des capacités des liens TE. Soit un réseau MPLS-TE sur WDM où chaque lien TE est un groupement de liens qui sont, dans ce cas, des canaux optiques. Le fonctionnement de MPLS DiffServ-TE n'est affecté que par la bande passante de chaque lien TE et cette dernière ne dépend que du nombre de canaux optiques regroupés et est indépendante de leur routage au niveau physique.

L'ajout des modèles DiffServ* et DiffProtect n'implique aucun changement majeur au fonctionnement de l'architecture MPLS-DiffServ TE. En effet, la topologie MPLS demeure intacte et seul le routage des liens composants des liens TE est affecté. Le flot de trafic entre deux LSR est déjà divisé parmi plusieurs liens composants et un algorithme de RWA normal établit ces liens composants sur le plus court chemin entre les LSR. Les modèles DiffServ* et DiffProtect proposent de séparer ces même liens composants sur des chemins disjoints.

4.3.5.1 MPLS DiffServ-TE et DiffServ*

La figure 4.7 montre le fonctionnement modulaire d'un routeur MPLS (LSR) dans un réseau MPLS DiffServ-TE. Un premier module (MPLS-TE) se charge d'admettre ou refuser les LSP selon leurs priorités et les classes de services auxquelles ils appartiennent. L'allocation de la bande passante du lien logique aux classes de service, et incidemment à leurs LSP respectifs, peut se faire selon plusieurs méthodes dont le *Maximum allocation Model (MAM)* (Faucheur, 2005a) ou le *Russian Dolls Model (RDM)* (Faucheur, 2005b). Pour MAM, les bandes passantes des CT sont séparées, alors que pour RDM, les bandes passantes sont partagées. La figure 4.7 illustre les deux stratégies. Avec RDM, la capacité réservée et non occupée par une classe de haute priorité peut être utilisée par une classe de priorité inférieure. Avec MAM, ce partage de capacité n'est pas possible.

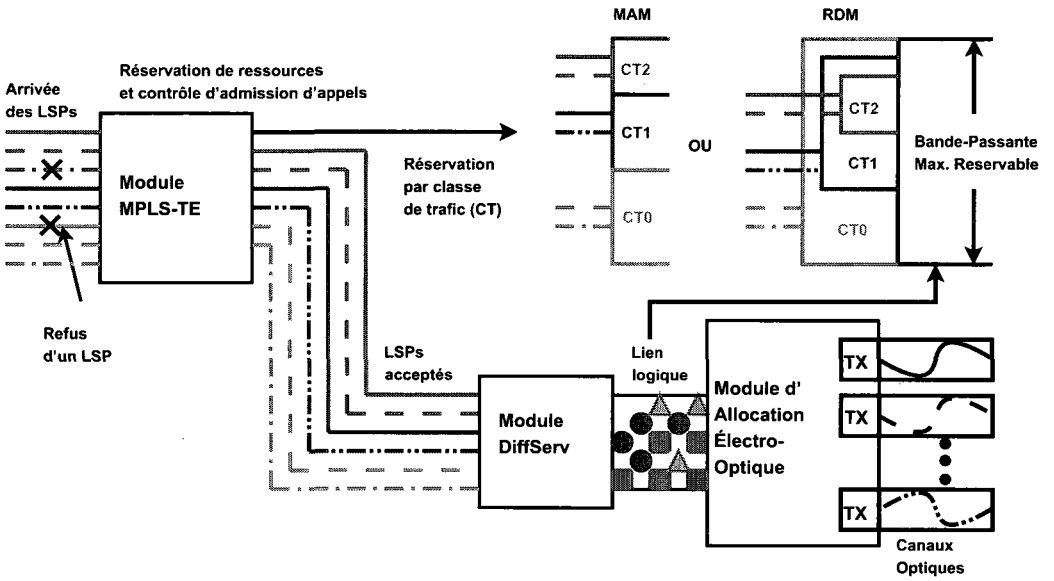


FIG. 4.7 MPLS DiffServ-TE : fonctionnement

Quand un LSP est admis dans un réseau MPLS, la bande passante qu'il requiert est réservée sur tous les liens qu'il traverse. Cette réservation est de type *soft*, ce qui signifie que le débit de trafic d'un LSP peut dépasser la limite réservée. Le module DiffServ est en place pour s'assurer que le débit de chaque classe de trafic demeure conforme à sa priorité et à la bande passante qui lui est réservée. Si le débit des différentes classes des LSP dépasse la capacité du lien logique, le module DiffServ assure un service différencié déterminé par la priorité EF, AF et BE des flots. Le débit du module DiffServ ne peut dépasser la capacité du lien logique auquel il est associé. Le trafic qui sort du module DiffServ subit une conversion électro-optique et est transmis physiquement vers le LSR adjacent. Comme le montre la figure 4.7, plusieurs canaux optiques peuvent être regroupés pour former le lien logique en question et pour satisfaire la demande de trafic entre une paire de LSR adjacents. Comme nous le montrons à la section 4.3.4 le partage de charge entre les chemins optiques se fait par LSP ce qui évite tout problème de désordre, car les paquets d'un même flot sont contraints à suivre le même chemin physique.

Si les canaux optiques sont routés sur le même chemin physique, une coupure de fibre en-

traîne une panne multiple de tous les canaux optiques qui la traversent. La communication entre les deux LSR adjacents est ainsi rompue. La bande passante maximale réservable de la figure 4.7 devient nulle, tout LSP traversant le LSR doit être rerouté sur un chemin secondaire et subir le processus d'admission de connexion et de réservation de ressource une deuxième fois avant d'être fonctionnel.

L'ajout du modèle DiffServ* ne change aucunement le fonctionnement des modules MPLS-TE, DiffServ et d'allocation électro-optique du trafic. Le changement exigé par ce modèle est au niveau WDM. Les canaux optiques d'un même groupement de liens sont séparés et routés sur des chemins optiques différents. Le partage du trafic se fait ainsi sur plusieurs canaux optiques physiquement disjoints.

Dans ce cas, une panne de fibre entraîne une diminution partielle de la bande passante du lien logique. Nous proposons plusieurs scénarios envisageables. La diminution de la bande passante du lien logique entraîne une diminution de la bande passante maximale réservable de la figure 4.7. Dans ce cas, un processus de restructuration de la réservation de ressources doit être déclenché. Le module d'allocation électro-optique déplace immédiatement les LSP du port en panne vers les autres et signale au module DiffServ de réduire son débit. Ce dernier assure une protection immédiate des trafics de hautes priorités en attendant l'accomplissement du processus de restructuration. Une fois achevé, un reroutage de certains LSP (surnuméraires) se fait s'il est requis. Le module MPLS-TE s'adapte à la nouvelle bande passante logique disponible et établit un procédé d'admission d'appels et réservation de ressources adéquat.

L'autre scénario sera de n'effectuer aucun changement au niveau de la bande passante maximale réservable de la figure 4.7. L'allocation des ressources (CT) reste la même, avant et après la panne. Dans ce cas :

- seuls les LSP affectés par la panne sont déplacés immédiatement vers les liens fonctionnels ;

- la capacité de transmission étant diminuée, le module DiffServ s'occupe de protéger le trafic prioritaire durant toute la durée de la panne ;
- le module MPLS-TE peut être informé de n'accepter aucun nouveau LSP pendant la durée de la panne ;
- aucune signalisation et reroutage global de LSP ne sont nécessaires.

Une description détaillée de ce comportement est donnée à la section 4.3.6. Il est toutefois possible de considérer un reroutage global seulement des LSP de basse priorité si la capacité résiduelle du reste du réseau le permet. Cette option est considérée dans l'étude de fiabilité de la section 4.4.

4.3.5.2 MPLS DiffServ-TE et DiffProtect

Dans le cas où DiffProtect est utilisé, certaines modifications structurelles sont nécessaires. La figure 4.8 montre un noeud MPLS DiffServ-TE adapté au modèle DiffProtect. Le module DiffServ est remplacé par un module DiffProtect qui se charge de séparer les flots de trafic selon leurs classes. Chaque classe de trafic est transmise sur des ressources optiques qui lui sont dédiées. La bande passante du lien logique est partagée de façon stricte par classe de service.

Le modèle d'allocation de ressources le plus appropriés dans le cas de DiffProtect est le MAM. Il y aura une association directe entre la bande passante réservée pour chaque CT et celle des canaux optiques réservés pour chaque classe de trafic. Plusieurs CT peuvent être inclus dans un même canal optique si la bande passante de ce dernier le permet. Quand la bande passante d'un CT dépasse celle d'un ou plusieurs canaux optiques, ces derniers seront réservés pour transporter seulement le trafic du CT en question. Dans l'une ou l'autre des possibilités, le trafic d'un CT doit utiliser un canal optique adéquatement protégé au niveau physique. Avec DiffProtect, la réservation *soft* des ressources de MPLS-TE devient

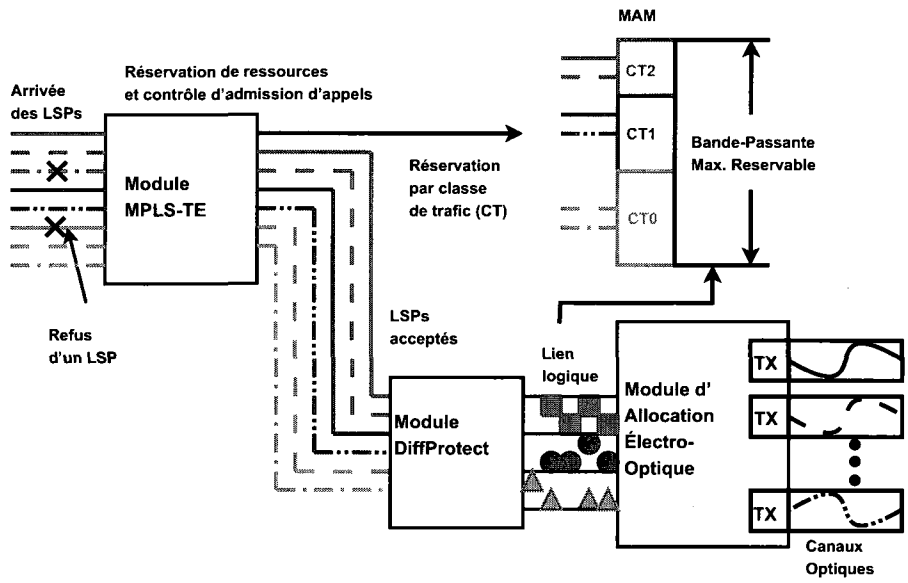


FIG. 4.8 MPLS DiffServ-TE : fonctionnement avec DiffProtect

stricte puisque les ressources de transmissions ne sont plus partagées. Les ressources de chaque classe de trafic sont garanties. Le module DiffServ n'est plus nécessaire puisque la contrainte de conformité de chaque flot aux ressources qui lui sont réservées est assurée physiquement.

4.3.6 Assignation optique du trafic dans un réseau MPLS-DS-TE

Cette section donne un exemple de fonctionnement complet d'un LSR-DiffServ* et d'un LSR-DiffProtect. Dans MPLS, les paquets qui ont une même étiquette et appartiennent à un même LSP, suivent tous le même chemin logique. Selon (Kompella et al., 2005), cette information est réutilisée pour définir aussi le chemin optique suivi par ces paquets. La figure 4.9 montre sous forme de diagramme modulaire, le fonctionnement complet d'un LSR avec DiffServ* ou DiffProtect.

Un classificateur à l'entrée du LSR détermine le LSP et la classe de service de chaque paquet qui arrive. Ce paquet est par la suite acheminé vers le port logique du lien TE

correspondant.

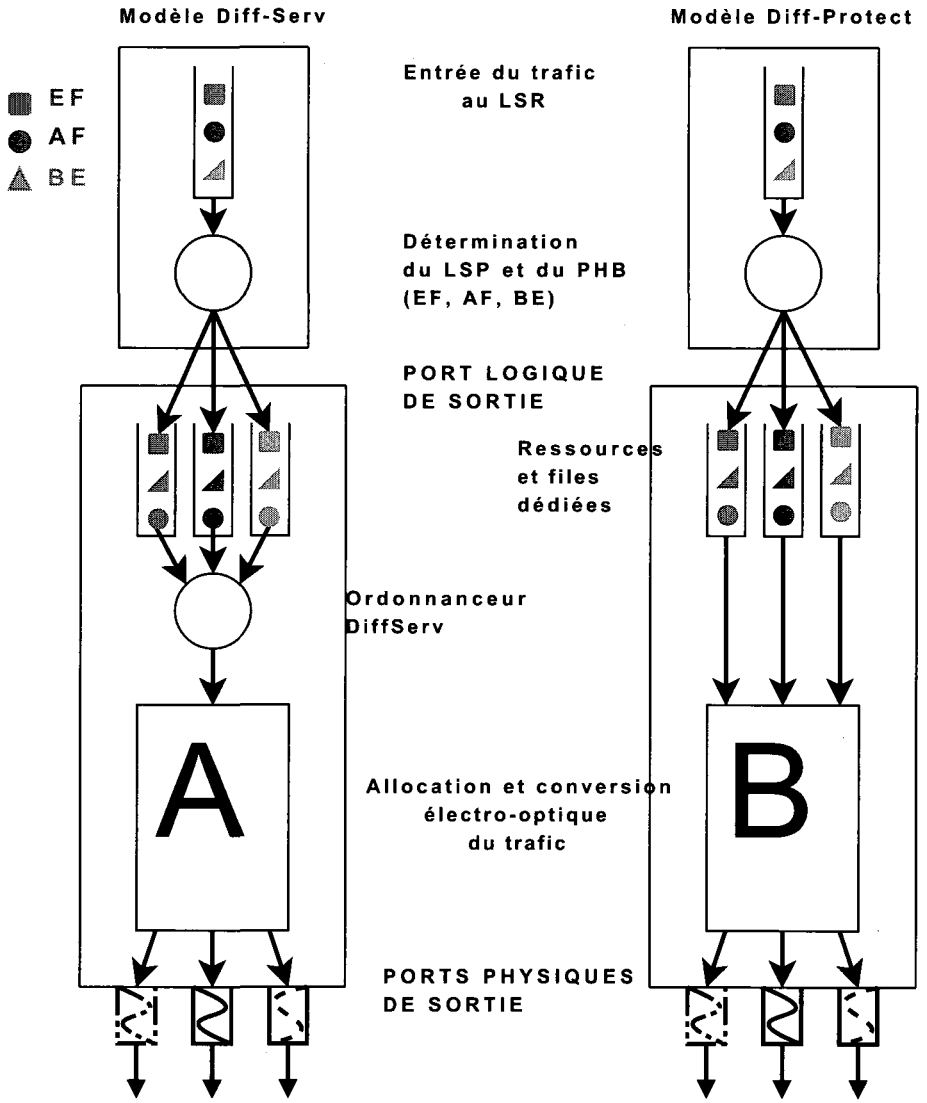


FIG. 4.9 LSR DiffServ*, DiffProtect

Chaque paquet est mis dans la file appropriée du port logique de sortie. Dans le cas de DiffServ*, un ordonnanceur DiffServ traite les paquets de façon prioritaire et ces derniers sont acheminés via un module de décision A qui acheminera le paquet vers un des ports physiques de sortie. Le fonctionnement du module A est illustré à la figure 4.10 et en cas de pannes, à la figure 4.11. Dans le cas de DiffProtect, les paquets sont acheminés par assignation directe via un module B vers le port de sortie approprié. Le fonctionnement

du module B est illustré à la figure 4.12.

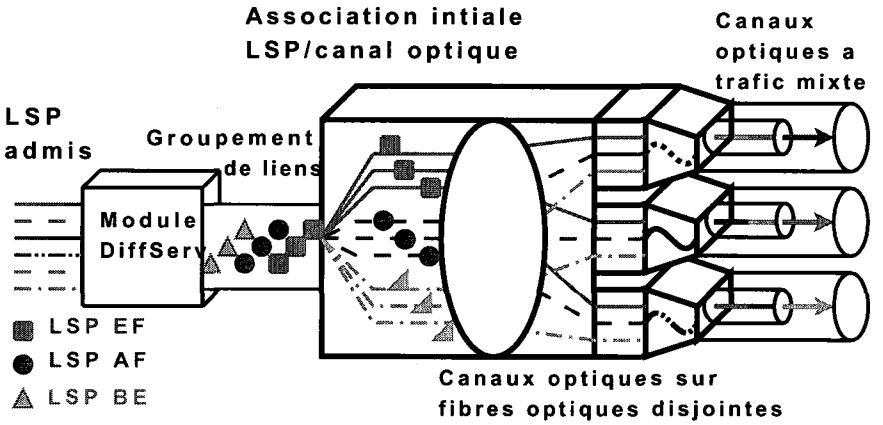


FIG. 4.10 DiffServ* : association LSP/canal optique

Nous supposons que le module A possède une table d'affectation <LSP-PortPhysique> prédéterminée par le module MPLS-TE de la figure 4.7. Cette affectation est aléatoire et dépend seulement de la bande passante disponible sur chaque lien optique. Dans le cas d'une panne d'un canal optique, une nouvelle affectation <LSP-PortPhysique> doit être mise en oeuvre. Le processus de réaffectation doit être aléatoire pour permettre au modèle DiffServ* de garantir un temps de réponse minimal en cas de pannes.

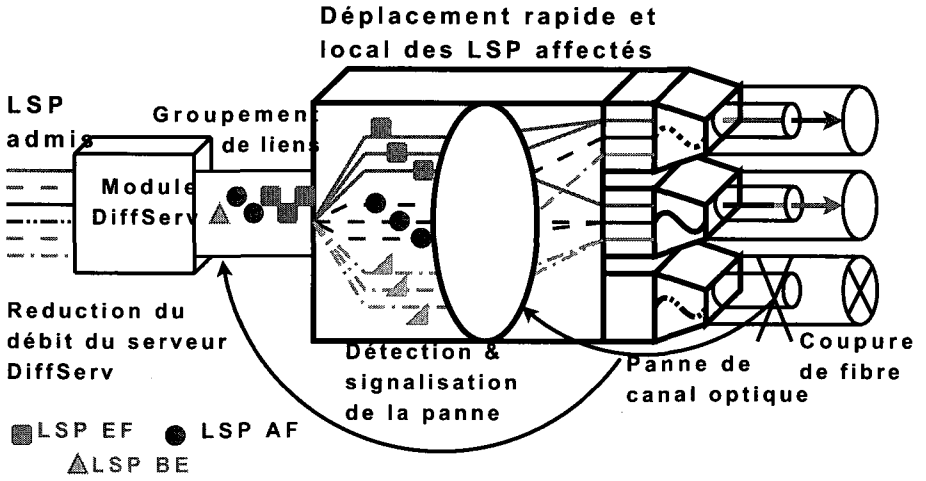


FIG. 4.11 DiffServ* : association LSP/canal optique suite après panne

En temps normal, le module A détermine le port de sortie de chaque LSP à partir de

l'élément <LSP-PortPhysique> de la table d'affectation correspondant. Dans le cas d'une panne d'un des canaux optiques, tous les éléments associés à ce port sont supprimés de la table. Plusieurs LSP ne seront plus assignés suite à la panne. Par phénomène de rétroaction, comme le montre la figure 1.7, le serveur DiffServ réduit son débit en fonction de la panne et le module d'assignation électro-optique se charge de créer une nouvelle entrée <LSP-PortPhysique (fonctionnel)> à l'arrivée du premier paquet d'un LSP non affecté.

Cette méthode permet d'éviter tout retard excessif dans la redirection des LSP affectés par la panne vers un des canaux optiques fonctionnels. Dans le cas d'une panne, l'interruption de service est réduite au temps de détection de la panne au niveau optique et de signalisation de cette panne aux modules logiques surjacents. Le reroutage d'un LSP est quasi immédiat puisqu'il se fait d'un port optique vers un autre au sein du même LSR. Aucun reroutage global n'est requis au niveau MPLS.

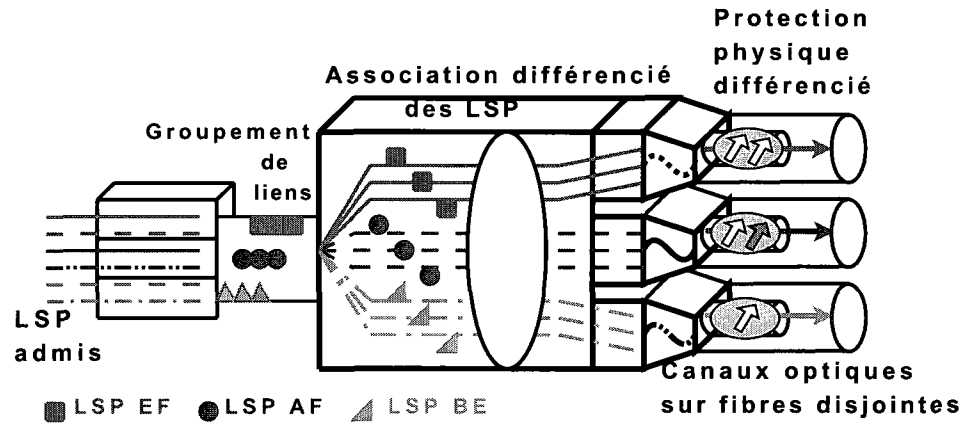


FIG. 4.12 DiffProtect : association LSP/canal optique

La figure 4.12 montre l'assignation directe du trafic qui se fait au sein du module *B* d'un LSR. Comme nous l'illustrons à la figure 4.13, toute occurrence de panne est traitée au niveau optique par les mesures de protection appropriées. Les LSP de la classe EF sont protégés à 100%, un canal de protection assure la transmission ininterrompue et complète du trafic suite à une panne. Le trafic AF n'est protégé que partiellement et il est possible dans ce cas de rerouter certains des LSP les plus affectés. Les LSP non protégés de basse

priorité pourront aussi être reroutés au niveau MPLS quand une panne touche le canal optique qui leur est réservé.

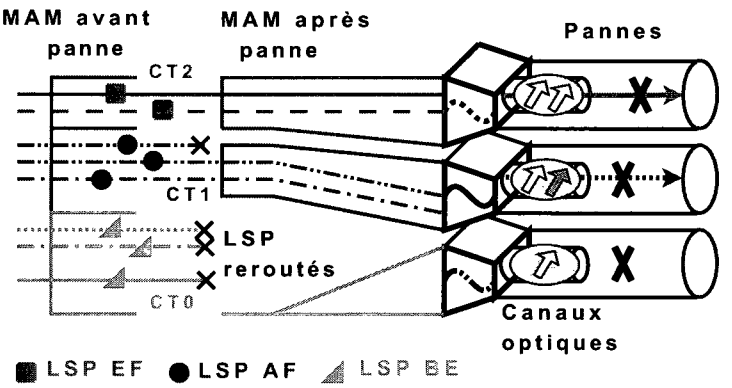


FIG. 4.13 DiffProtect : association LSP/canal optique après panne

Il est possible de voir à l'aide des figures 4.14 et 4.15 l'assignation électro-optique des LSP et l'effet d'une coupure de fibre dans ce cas. Pour un réseau MPLS-DS-TE normal, les canaux optiques d'un même lien TE ne doivent pas être disjoints et peuvent être mis en place sur le même chemin physique. Dans ce cas, une coupure de fibre provoque la panne de tous les canaux optiques et donc du lien TE correspondant ; tous les LSP qui étaient assignés à ce port logique de sortie doivent être reroutés.

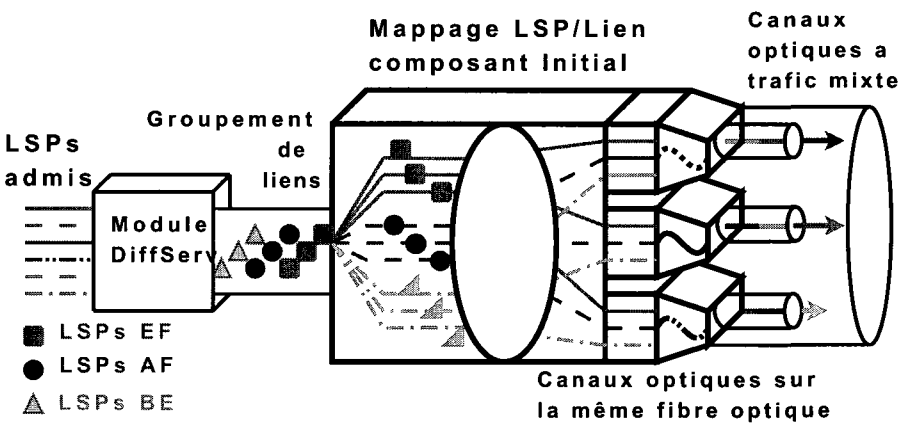


FIG. 4.14 MPLS standard : association LSP/canal optique

Nous pouvons donc conclure que MPLS-DS-TE possède tous les outils nécessaires pour

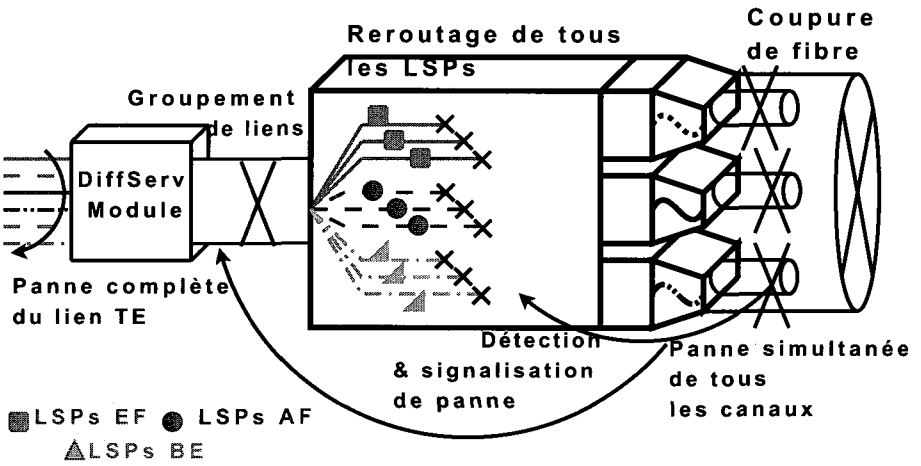


FIG. 4.15 MPLS standard : association LSP/canal optique après pannes

assurer une intégration facile de DiffServ* et avec certaines petites modifications, DiffProtect. DiffServ* se base sur un déplacement des LSP touchés par la panne vers les canaux optiques fonctionnels et assure, à l'aide du module DiffServ, une protection adéquate du trafic prioritaire. DiffProtect ne requiert aucun changement de l'affectation électro-optique des LSP à l'issue d'une panne mais traite ses conséquences directement au niveau physique.

4.4 Fiabilité des réseaux MPLS-DS-TE

Nous avons dans les sections précédentes :

- décrit le déploiement des modèles DiffServ* et DiffProtect dans des réseaux MPLS-DS-TE ;
- expliqué qualitativement comment l'ajout des deux modèles peut améliorer la fiabilité de MPLS-DS-TE dans des conditions de pannes simples et mêmes multiples.

Nous présentons dans cette section des résultats de simulations qui appuient nos hypothèses et qui démontrent effectivement que l'ajout seul de DiffServ* permet d'augmenter la résilience et la performance des réseaux MPLS-DS-TE en cas de pannes.

Nous simulons pour notre étude, le réseau des parties supérieures des figures 4.1 et 4.2. Ce réseau est composé de :

- quatre LSR 1, 2, 3 et 4 ;
- une topologie logique telle que trois chemins disjoints sont disponibles entre les LSR 1 et 2 :
  - tous les liens de la couche logique sont des groupements de trois canaux optiques ;
- le réseau de la figure 4.1 est simulé pour étudier la fiabilité de MPLS-DS-TE dans le cas standard ou régulier ;
- le réseau de la figure 4.2 est simulé pour étudier la fiabilité de MPLS-DS-TE avec DiffServ*.

Comme nous l'avons démontré à la section 4.1, un lien TE logique protégé par DiffServ* est plus robuste puisqu'une coupure de fibre optique ne peut causer par elle-même la rupture totale de la communication entre les LSR adjacents. Ceci est mis en évidence dans la figure 4.16 dans laquelle nous montrons l'effet d'une panne de lien physique sur la topologie logique. Remarquons que dans les cas des deux techniques de groupement de liens, régulière et DiffServ* :

- aucune protection optique n'est disponible ;
- un lien physique qui tombe en panne reste dans cet état jusqu'à sa réparation ;
- dans le cas de déploiement régulier, la panne du lien $[C1, C2]$:
  - induit la panne simultanée des trois composantes optiques de $(LSR1, LSR2)$,
  - possède un effet *localisé* (c.f. le côté gauche de la figure 4.16),
  - cause la rupture complète de toute communication directe entre les LSR 1 et 2 ;
- dans le cas de MPLS-DS-TE avec DiffServ* :
  - trois chemins optiques de trois liens logiques différents traversent le lien physique $[C1, C2]$,
  - en cas de coupure de la fibre optique entre $C1$ et $C2$:
    - l'effet de la panne est *distribué*,

- trois liens logiques, $(LSR1, LSR2)$, $(LSR1, LSR3)$ et $(LSR3, LSR2)$ sont affectés,
- l'effet de la panne est seulement partiel puisque seul un des chemins optiques des liens mentionnés est touché,
- la panne cause une réduction de la bande passante partielle au niveau des trois liens logiques.

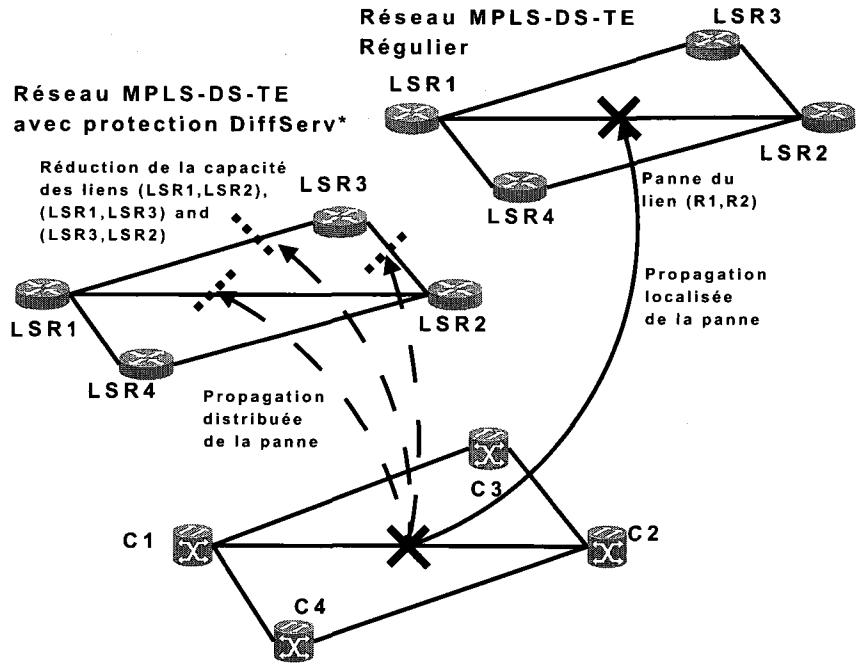


FIG. 4.16 Propagation de panne localisée VS distribuée

En somme, DiffServ* permet à plusieurs liens TE de partager un effet *réduit* de la panne physique. Nous comparons ceci au cas régulier dans lequel un lien-faisceau subit les conséquences complètes de cette même panne.

Nous illustrons à la figure 4.17 la réaction du réseau MPLS-DS-TE dans les deux cas régulier et DiffServ*. Pour MPLS-DS-TE standard, le lien $(LSR1, LSR2)$ tombe en panne, les mécanismes de protection de MPLS sont déclenchés et les LSP qui traversent le lien en faute sont reroutés. Le processus de reroutage est :

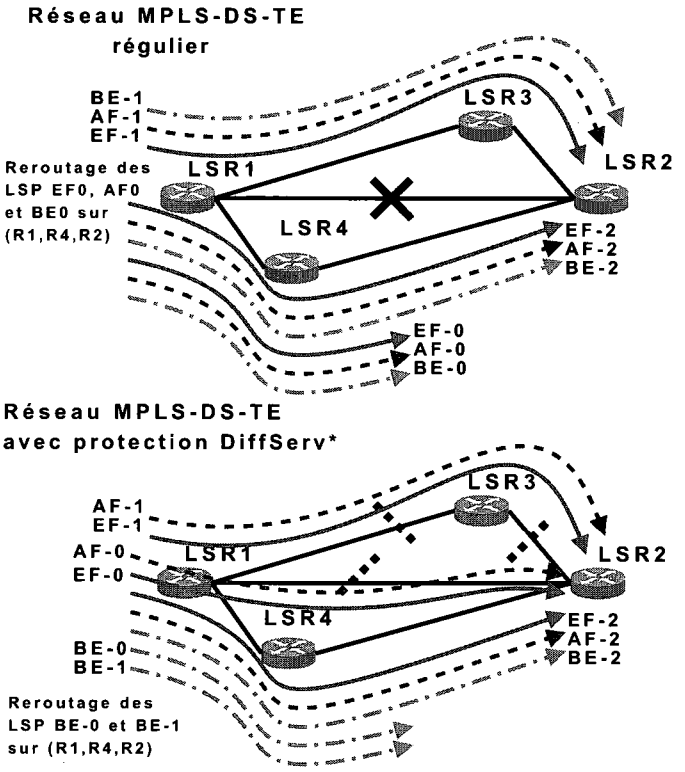


FIG. 4.17 Retourage des LSP en cas de panne

- Immédiat pour les LSP qui sont déjà assignés à des chemins de secours précalculés.
- Plus lent si des LSP de secours doivent être mis en place en temps et lieu après la panne.
- Dans ce cas, le temps de rétablissement de service dépend de :
  - La priorité des LSP considérés pour le reroutage
  - La capacité résiduelle disponible à d'autres parties du réseau.

Dans le cas de DiffServ*, nous n'observons aucune panne de lien au niveau logique. La coupure de fibre cause une réduction partielle de la bande passante de certains des liens TE. Ceci résulte en une congestion et c'est le module DiffServ qui assure une protection locale et immédiate ainsi qu'un service adéquat aux flots de hautes priorités, et ce, sans recours à aucun reroutage. Il est cependant clair que la dégradation de performance en cas de panne sera plus ardue pour les flots de basses priorités. Étant donné que le reroutage de flots est beaucoup plus facile à réaliser dans les réseaux MPLS-DS-TE, il est alors possible d'en profiter pour rerouter les LSP BE de façon à éviter les régions affectées par la panne et possiblement leur assurer un meilleur service.

4.4.1 Simulation

La configuration et les caractéristiques de la simulation réalisée pour cette étude sont décrites. Dans ce qui suit :

- l'expression *protection MPLS* désigne un réseau MPLS-DS-TE normal qui :
  - n'utilise pas DiffServ*,
  - ne possède que les mécanismes de reroutage MPLS pour protéger le trafic en cas de panne ;
- évidemment l'expression "protection DiffServ*" désigne celle qui utilise, en plus, Diff-Serv*.

4.4.1.1 Les flots du réseau

La topologie logique simulée est celle de la figure 4.17 et le trafic qui la traverse est décomposé comme suit :

- les LSP EF0, AF0 et BE0 appartiennent au flot 0 et sont mis en place sur le chemin $(LSR1, LSR2)$:
  - le flot 0 est touché par la panne quelle que soit la technique de protection utilisée :
    - l'effet est seulement partiel avec DiffServ*,
    - la rupture est totale dans le cas de la configuration régulière ;
- les LSP EF1, AF1 et BE1 font parties du flot 1 et sont mis en place sur le chemin $(LSR1, LSR3, LSR2)$:
  - le flot 1 est seulement affecté dans le cas de DiffServ* et l'effet est partiel ;
- EF2, AF2 et BE2 sont les LSP du flot 2 et sont mis en place sur $(LSR1, LSR4, LSR2)$:
  - à cause du processus de reroutage, la panne touche indirectement le flot 2 :
    - dans le cas standard, tous les LSP du flot 0 sont reroutés sur $(LSR1, LSR4, LSR2)$,
    - seuls les LSP BE des flots 0 et 1 sont rerouté sur ce chemin dans le cas de Diff-Serv*.

4.4.1.2 Les sources de trafic

Les sources de trafic utilisés dans cette étude sont les mêmes que celles des études du chapitre précédent :

- des sources de VoIP sont utilisés pour le trafic EF ;
- des sources vidéo MPEG4 génèrent le trafic AF ;
- des sources on-off exponentielles sont utilisés pour simuler le trafic de données de la classe BE.

La capacité totale disponible sur chaque lien logique du réseau est de 15 Mbps soit 5 Mbps par composante optique. La bande passante requise par le trafic des classes EF, AF et BE est la même sur les chemins $\{LSR1, LSR2\}$ et $\{LSR1, LSR3, LSR2\}$. Chacun des LSP EF, AF et BE des flots 0 et 1 requiert près de 5 Mbps ce qui produit un taux d'utilisation élevé d'approximativement 80% sur ces deux chemins. Le débit des sources qui génèrent le trafic du flot 2 est différent des deux premiers et nous justifions ceci dans ce qui suit.

4.4.1.3 Le scénario de pannes

Dans le cas de la protection MPLS, le lien logique $(LSR1, LSR2)$ tombe complètement en panne suite à la coupure de fibre $[C1, C2]$. La capacité de transmission totale entre $LSR1$ et $LSR2$ est réduite de 45 Mbps à 30 Mbps et tous les LSP déjà établis sur ce chemin doivent être reroutés.

Dans le cas de DiffServ*, la panne du lien physique $[C1, C2]$ diminue du tiers la bande passante de plusieurs liens TE. Dans ce cas, la capacité de transmission totale perdue entre les LSR 1 et 2 est de 10 Mbps et seuls les LSP de basse priorité sont reroutés.

4.4.1.4 Reroutage des LSP et capacité résiduelle du réseau

Dans les deux cas de la protection MPLS et DiffServ*, nous utilisons les capacités de reroutage de MPLS pour tenter de rétablir un meilleur service aux LSP les plus pénalisés par la panne. Dans les deux cas, les LSP sont reroutés sur le troisième chemin $\{LSR1, LSR4, LSR2\}$ qui :

- représente le reste du réseau qui n'est pas touché par la panne ;
- définit la capacité résiduelle du réseau disponible pour servir les LSP reroutés ;
- indique la quantité de bande passante disponible donc le niveau de congestion qui peut

avoir lieu suite au reroutage des LSP touchés par la panne ;

Les conséquences sur la performance sont variables selon la charge du réseau. Nous étudions la performance des deux méthodes de protection pour différentes capacités résiduelles soit, 80%, 60%, 40% et 20% sur le chemin $(LSR1, LSR4, LSR2)$.

Dans le cas de la protection MPLS :
- les LSP EF0, AF0 et BE0 sont reroutés sur le chemin $(LSR1, LSR4, LSR2)$;
- tous les LSR sur ce chemin sont configurés avec DiffServ et doivent donc être capable de traiter ce supplément de trafic.

Toutefois, si la nouvelle demande de trafic sur ce chemin dépasse les limites de garanties de service configurées, il est possible d'observer une dégradation de la qualité de service même pour les flots de hautes priorités.

Quand DiffServ* est utilisé, un chemin optique est perdu sur $(LSR1, LSR2)$, un autre sur $(LSR1, LSR3, LSR2)$. La bande passante restante sur ces chemins suffit à servir adéquatement les flots EF et AF de haute et moyenne priorité et seuls les LSP BE0 et BE1 sont reroutés sur le troisième chemin. Dans ce scénario :
- les flots EF et AF reçoivent un service adéquat ;
- selon la capacité résiduelle sur le troisième chemin, les flots BE subissent certaines dégradations de qualité de service.

4.4.2 Résultats

Cette section montre les résultats des simulations. Le réseau a été étudié dans les deux cas de protection DiffServ* et MPLS tout en considérant une capacité résiduelle variable sur le troisième chemin $(LSR1, LSR4, LSR2)$ dans les deux cas. Nous évaluons la performance des deux méthodes par le taux de pertes des paquets, le délai moyen et la gigue pour les classes EF, AF et BE dans les deux situations normales et sous pannes.

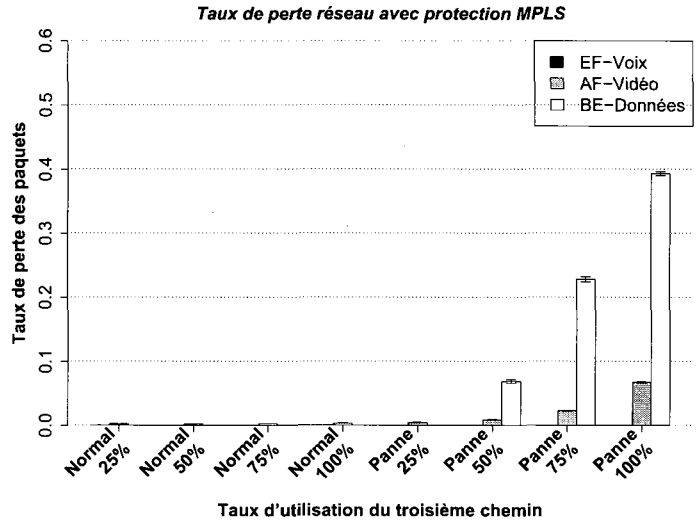
Les figures 4.18, 4.19 et 4.20 montrent la moyenne sur l'ensemble du réseau et en cas de pannes du taux de pertes, du délai et de la gigue des trois flots 0, 1 et 2. Les résultats individuels pour chaque flot sont montrés dans l'annexe IV. Nous pouvons voir qu'en cas de fonctionnement normal, la performance moyenne du réseau est identique dans les deux cas de le protection MPLS et DiffServ*. Ceci est normal vu que le comportement des deux réseaux diffère seulement en cas de pannes. Dans ce qui suit, nous mettons en évidence la différence en performance en cas de pannes.

Nous pouvons voir des figures 4.18(a) et 4.18(b) qu'en moyenne la performance de Diff-Serv* est meilleure que celle de la protection MPLS. Avec DiffServ* :

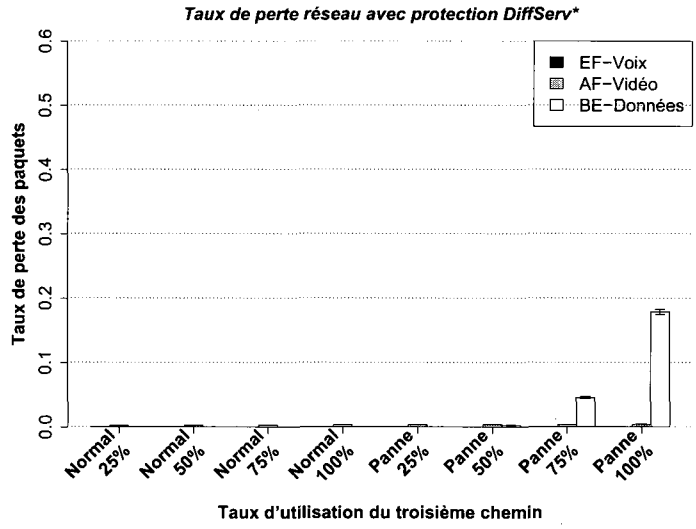
- les LSP EF et AF des flots 0 et 1 ne sont pas reroutés suite à la panne :
  - la bande passante résiduelle sur leurs chemins d'origine est réduite,
  - mais elle reste suffisante pour assurer un service convenable ;
- les LSP BE de ces flots sont rétablis sur le troisième chemin :
  - la surcharge de trafic non prioritaire n'affecte pas les LSP EF et AF du flot 3,
  - elle affecte seulement BE quand la demande de trafic sur ce chemin est élevée.

Dans le cas de la protection MPLS, le flot 1 n'est pas touché par la panne et le flot 0 est rerouté sur le même chemin que le flot 2. La performance de ces deux flots dépend intrinsèquement de la capacité résiduelle originale du troisième chemin et donc du niveau de congestion engendré par la surcharge de trafic à la fois EF, AF et BE sur ce chemin. Les conclusions sur le taux de pertes moyen pour les différentes classes de trafic sont :

- trafic EF : même niveau de protection dans les deux cas ;
- trafic AF : le taux de pertes est réduit à des valeurs presque nulles dans le cas de Diff-Serv* ;
- trafic BE : le taux de pertes est double avec la protection MPLS ;
- de très grands taux de pertes, près de 10% des paquets AF et 40% des paquets BE sont observés avec MPLS quand la capacité résiduelle du réseau est de 20%.



(a) Cas normal vs en panne, Protection MPLS



(b) Cas normal vs en panne, Protection DiffServ*

FIG. 4.18 Taux de pertes moyen du réseau

Les figures 4.19(a) et 4.19(b) indiquent que le délai moyen des classes EF et AF sont similaires dans les deux cas des protection DiffServ* et MPLS, celui de la classe BE est meilleur dans le premier cas. Avec DiffServ*, la réduction de la bande passante des chemins des flots 0 et 1 :

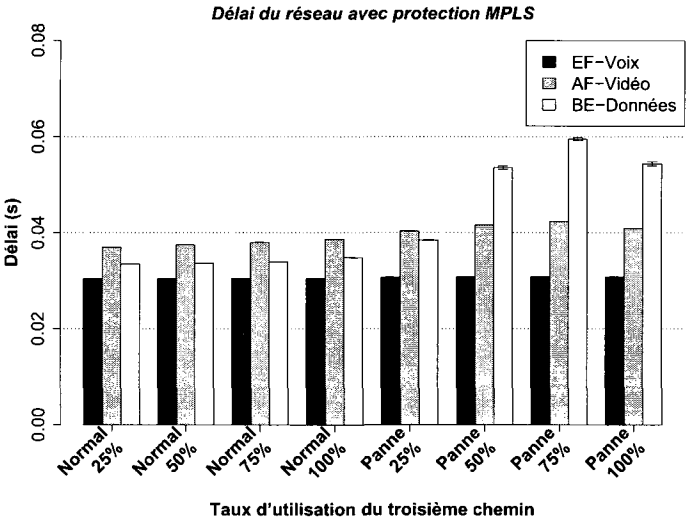
- n'a aucun effet significatif sur le délai EF mais cause une légère augmentation dans le cas de AF :
  - ceci est principalement dû à la taille et à la transmission en rafales des paquets AF de la source vidéo ;
- l'augmentation du délai dans le cas de BE est proportionnel au taux d'utilisation original du troisième chemin $\{LSR1, LSR4, LSR2\}$.

Dans le cas de MPLS, le flot 1 n'est pas touché par la panne et conserve les mêmes valeurs de délai avec et sans pannes. La situation diffère pour les flots 0 et 2 qui sont maintenant en compétition pour les ressources de plus en plus limitées du troisième chemin d'où une augmentation du délai. L'augmentation du délai des paquets BE est plus grande avec MPLS puisque ces paquets sont maintenant en compétition avec une plus grande quantité de trafic EF et AF pour les mêmes ressources du troisième chemin de protection. Les taux des pertes des paquets AF et BE élevés dans le cas 20% de la protection MPLS permettent d'expliquer la décroissance du délai moyen dans ce cas.

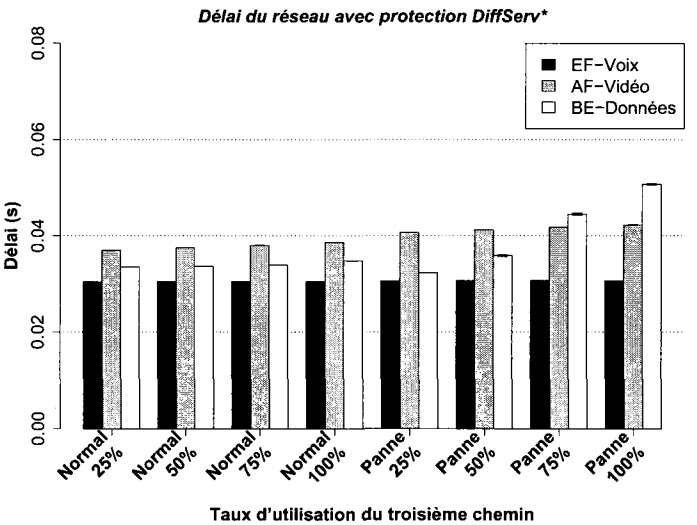
Les résultats pour la gigue sont comparés à l'aide des figures 4.20(a) et 4.20(b). La gigue moyenne du trafic AF est légèrement meilleure avec MPLS, celle du trafic BE est plus basse avec DiffServ* et la gigue des paquets EF est la même dans les deux cas.

Avec DiffServ* et pour les mêmes raisons que le délai moyen :

- les valeurs de gigue des paquets AF des flots 0 et 1 sont doubles quand la bande passante de leurs chemins respectifs est réduite suite à la panne ;
- la gigue AF du flot 2 reste la même et les flots additionnels ajoutés sur ce chemin sont BE :



(a) Cas normal vs en panne, Protection MPLS

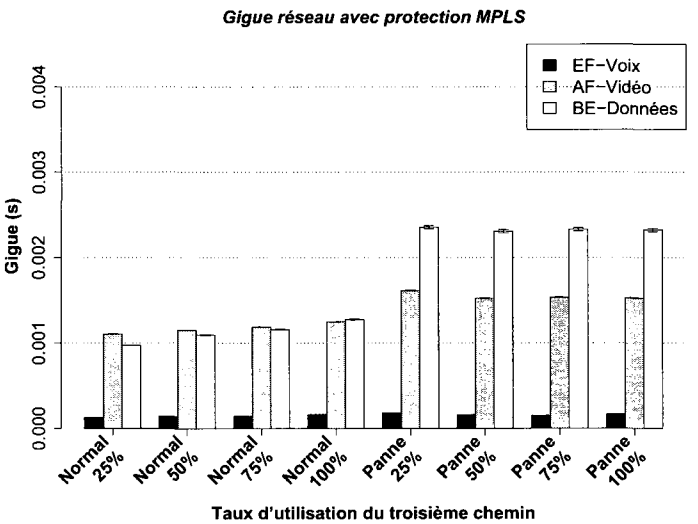


(b) Cas normal vs en panne, Protection DiffServ*

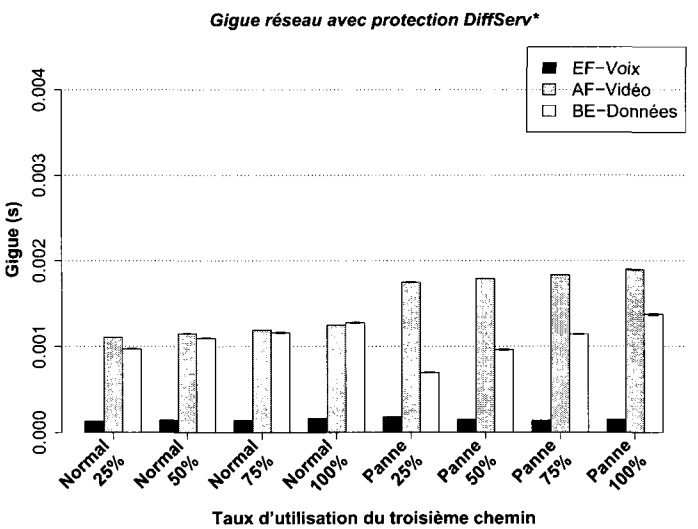
FIG. 4.19 Délai moyen du réseau

  - ils n'affectent pas les paquets des autres classes ;
- la gigue des paquets BE est meilleure avec DiffServ* et ceci est principalement dû aux quantités plus faibles du trafic EF et AF sur le troisième chemin comparé à MPLS.

Avec MPLS, le flot 1 n'est pas touché par la panne donc aucune dégradation de performance n'est observée. D'un autre côté, la gigue des paquets AF et BE des flots 0 et 2 est plus haute, mais constante en cas de pannes et quel que soit le niveau d'utilisation du réseau. Ces résultats confirment notre analyse qualitative sur l'amélioration qu'apporte DiffServ* sur la fiabilité et la performance des réseaux MPLS-DS-TE. Avec DiffServ*, l'effet de la panne est distribué sur plusieurs groupements de liens logiques donc sur plusieurs flots, ce qui minimise l'impact des pannes physiques sur la couche de service supérieure. Les flots de hautes priorités ne sont pas touchés dans toutes les conditions et seul le trafic BE doit être rerouté en fonction de la capacité résiduelle.



(a) Cas normal vs en panne, Protection MPLS



(b) Cas normal vs en panne, Protection DiffServ*

FIG. 4.20 Gigue moyenne du réseau

CHAPITRE 5

DÉPLOIEMENT

DiffServ* se base sur deux éléments essentiels pour assurer une protection différenciée et adéquate du trafic en cas de pannes dans un réseau. Le premier est l'architecture des services différenciées, DiffServ, qui peut protéger le trafic prioritaire en cas de congestion des liens de la couche logique. Le second est la technique d'agrégation de liens, qui permet de grouper plusieurs canaux de transmissions physiques en un lien logique de capacité supérieure. La combinaison des deux éléments doit *en théorie* faire de DiffServ* un modèle *fonctionnel* puisqu'une panne physique se traduirait en une congestion sur des liens de la couche logique et ne nécessiterait rien de plus que les mécanismes naturels de DiffServ pour protéger le trafic en fonction de sa classe de priorité.

Étant donné que les simulations ont déjà démontré l'efficacité du modèle DiffServ* théorique, nous avons procédé en validant sa faisabilité et sa performance en laboratoire à l'aide d'équipement de communication actuellement disponible. Ceci est d'une grande importance puisque ça complète notre proposition et permet de l'ajouter au gabarit des modèles de protection différenciée efficaces des réseaux de prochaines générations. L'objectif de ce chapitre est alors de montrer que :

- il est *en pratique* possible de déployer DiffServ* à l'aide de tout équipement réseau qui permettrait de combiner la différenciation de services avec la technologie d'agrégation de liens ;
- DiffServ* est effectivement capable de protéger le trafic prioritaire en cas de *vraies* pannes physiques dans un réseau *réel* et avec des équipements actuellement disponibles sur le marché.

5.1 DiffServ* et type de réseau visé

Le modèle DiffServ* a été initialement élaboré pour être déployé dans des réseaux IP/WDM de prochaines générations. Ces réseaux contiennent tous les éléments de base nécessaires au bon fonctionnement de DiffServ* et, si la situation le requiert, DiffProtect. L'évaluation de la performance de DiffServ* et de DiffProtect au cours des chapitres précédents a été réalisée en simulant une couche logique protégée par l'un, l'autre ou une combinaison des deux modèles. La topologie physique dans la simulation n'a été prise en compte qu'indirectement puisque nous ne tenions compte que de *l'effet* qu'ont les pannes physiques sur la couche logique. Ceci permet de montrer que la performance et la fiabilité de DiffServ* n'est pas reliée à une infrastructure physique particulière mais seulement à la possibilité d'agrégation de liens qu'une telle couche peut offrir.

Dans le cadre de cette étude nous avons décidé de déployer DiffServ* dans un réseau de type IP/Ethernet. Ces réseaux ont la particularité d'être moins chers et techniquement plus faciles à utiliser que les réseaux optiques. Par exemple, nous savons que la capacité de transmission actuelle d'un canal optique se chiffre en gigabits et en dizaine de gigabits par seconde. Il serait alors pratiquement impossible de générer une telle quantité de trafic en laboratoire et les réseaux Ethernet de plus basses vitesses sont alors mieux adaptés à ce contexte.

Ethernet est une technologie réseau très populaire et pratiquement la plus utilisé dans la mise en place des réseaux régionaux locaux (Local Area Network, LAN) et certains réseaux métropolitains (Metropolitan Area Network (MAN)). Cette technologie répond à nos besoins puisqu'elle permet, par l'entremise du Link Agregation Control Protocol (LACP) (lac, 2002) défini par le standard d'agrégation de liens IEEE802.3ad (IEEE, 2000), de regrouper des liens Ethernet pour former un conduit logique de plus grande capacité. Cette pratique est courante dans les réseaux Ethernet car elle permet d'augmenter la capacité de transmission des liens qui relient deux équipements réseaux. Dans le cas

des réseaux Ethernet multiservices, l'ajout de DiffServ* peut s'avérer souhaitable pour assurer la fiabilité et la protection différenciée de trafic.

5.2 Description de l'expérience et des équipements réseaux nécessaires

L'objectif principal de cette expérience est de valider la fonctionnalité et la performance du modèle de protection DiffServ* dans un réseau réel. Nous voulons montrer que DiffServ* peut effectivement garantir la qualité de service des applications dans une situation de panne réelle. Nous avons mis en place le réseau de la figure 5.1. Le réseau dorsal est composé de deux commutateurs Cisco de type Catalyst 3750E-24-TD, surnommés Atlas et Hercules et réliés par un *Etherchannel*. Cette technique de groupement de liens est l'implémentation du LACP et une technologie de Cisco. De part et d'autre du réseau dorsal nous avons deux réseaux locaux d'ordinateurs qui serviront de générateurs, de récépteurs et d'analyseurs de trafic. Les machines du réseau A génèrent et transmettent en direction du réseau B trois types de trafic EF, AF et BE à un débit suffisamment grand pour saturer la capacité de l'Etherchannel qui les relie. Toute panne dans ce groupement de liens entraîne la diminution de la capacité de transmission disponible entre les réseaux A et B et les effets de la panne seront mesurables à l'arrivée au réseau B.

5.2.1 Générateurs et analyseurs de trafic

Nous avons généré trois types de trafic pour trois classes distinctes, du trafic de voix sur IP (VoIP) classifié EF, du trafic de vidéo AF et du trafic UDP de données pour BE. Le trafic EF et BE a été généré par le logiciel Distributed-Internet Traffic Generator (D-ITG) (Botta et al., 2007). Le trafic AF est généré par un logiciel de transmission vidéo, le VLC media player (VideoLAN Project, 2009).

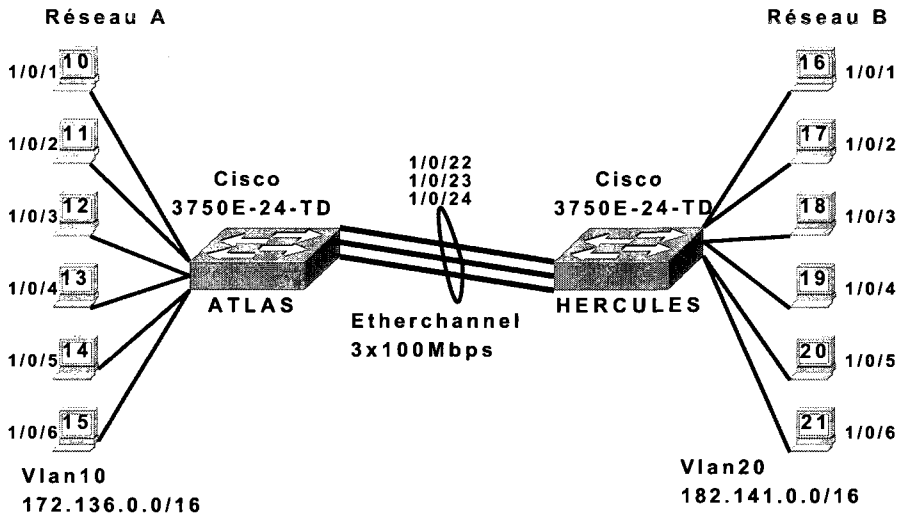


FIG. 5.1 Réseau Etherchannel

Classe	Type de trafic	Nombre de sources	Débit moyen par source	Débit total
EF	Voix sur IP	130	108 kbps	14.04 Mbps
AF	Transmission vidéo	2	6.5 Mbps	13 Mbps
BE	Données (UDP)	4	4.14 Mbps	16.56 Mbps

TAB. 5.1 Sources et débit de trafic par machine

L'objectif est de saturer la capacité totale de l'Etherchannel de 300 Mbps. Pour reproduire des conditions similaires à celles des études par simulation de DiffServ*, les différentes catégories de trafic partagent à parts égales la capacité de transmission totale disponible. Ainsi, la totalité de trafic EF, AF *ou* BE qui circule du réseau A vers B doit être proche, mais ne doit pas dépasser, la limite de 100 Mbps.

Le tableau 5.1 montre la composition du trafic généré par chacune des machines du réseau A ainsi que le débit total par source de chaque catégorie. Du trafic de voix sur IP forme la classe EF. Chaque source de voix utilise l'encodage G711.1 et génère un débit constant de 108 kbps de trafic, incluant toutes les entêtes de transmission du réseau. Chaque machine du réseau A utilise 130 de ces sources et génère un total de 14 Mbps. Deux sources vidéo génèrent le trafic AF de débit variable qui tourne autour de 6.5 Mbps.

Chaque poste du réseau A génère au total 13 Mbps de trafic AF. Finalement quatre sources de données sont utilisées pour générer le trafic de basse priorité BE. Chacune génère un débit constant de 4.14 Mbps, pour un total 16.56 Mbps par machine. Les graphiques des figures 5.2 et 5.3 montrent un exemple du débit de trafic généré par une machine source du réseau A et reçu par une machine destination du reseau B.

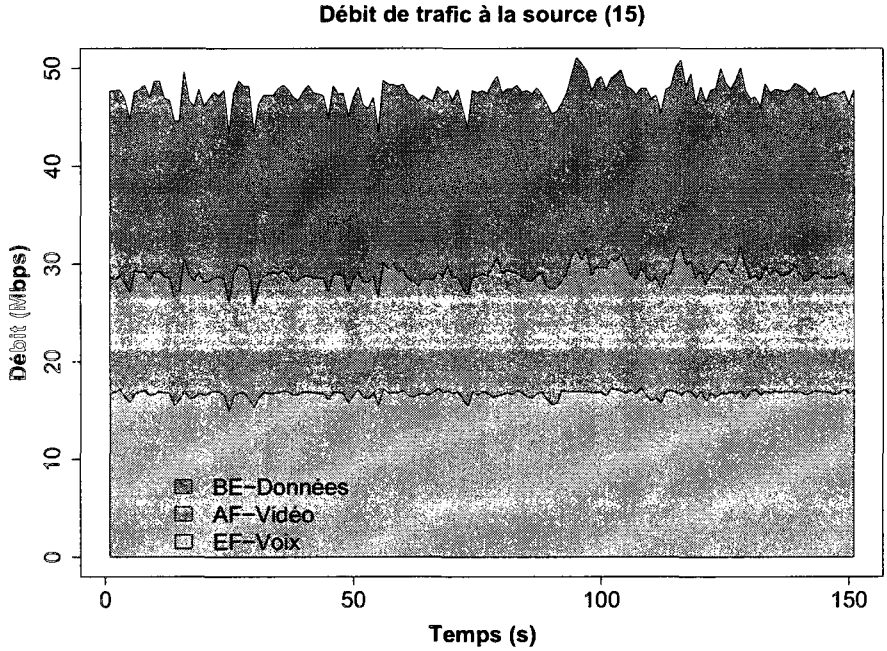


FIG. 5.2 Débit normal de trafic EF, AF et BE

Les 6 machines du réseau A sont identiquement configurées et nous avons alors en moyenne un total de 84.24 Mbps de trafic EF, 78 Mbps de trafic AF et 99.36 Mbps de trafic BE qui traversent l'Etherchannel entre les réseaux A et B. Le total étant en moyenne de 261.6 Mbps, la panne d'un des liens de l'Etherchannel réduit sa bande passante de 300 à 200 Mbps. Ceci entraîne une congestion et l'activation des mesures de qualité de service dans cette partie du réseau.

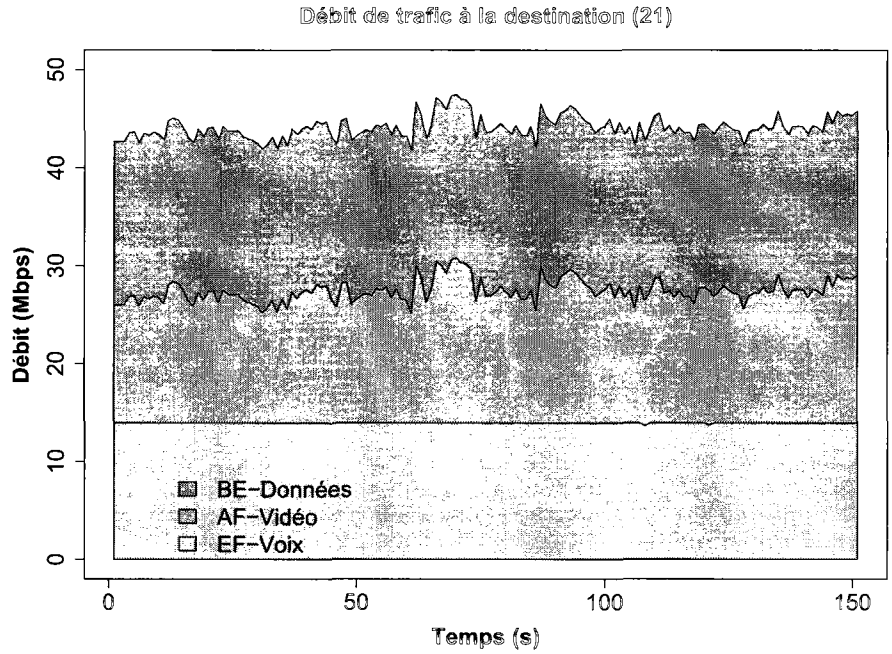


FIG. 5.3 Débit normal de trafic EF, AF et BE

5.2.2 Configuration des commutateurs Atlas et Hercules.

Nous avons choisi la série Cisco Catalyst 3750E-24-TD pour plusieurs raisons. Ces équipements sont capables de différenciation de service, c'est-à-dire, peuvent classifier, surveiller, marquer, mettre en files d'attente et ordonnancer leur service pour assurer un traitement de trafic prioritaire en cas de congestion. En second lieu, ils peuvent agréger des liens Ethernet pour former un canal logique de plus grande capacité. Et finalement, parce qu'il est possible d'appliquer des mesures de qualité de service autant sur des ports physiques individuels que sur des groupements de liens, ce type de réseau répond aux critères de base de la protection DiffServ*.

Il existe cependant certaines différences entre le modèle DiffServ* théorique tel que nous le proposons et l'implémentation pratique réalisée à l'aide des commutateurs Cisco. Cette différence est illustrée à la figure 5.4. Dans la partie du haut, nous pouvons voir le fonctionnement de la proposition DiffServ* théorique dans laquelle le trafic de chaque classe

de service, essentiellement EF, AF et BE, est mis en attente dans une file qui lui est propre. Un ordonnanceur se charge de servir chaque file en fonction de sa priorité et le trafic sort de ce dernier à un débit inférieur ou égal à la capacité totale du groupement logique de liens et est divisé par la suite de façon équilibrée sur les ports de transmission sous-jacents. L'ordonnanceur est prioritaire, c'est-à-dire que la file associée au trafic AF n'est servie que quand la file EF est vide, la file BE n'est servie que quand les files EF et AF sont vides. Cette configuration est nécessaire parce qu'elle permet de préserver, autant que possible, le même taux de service aux flots de hautes priorités, en cas de pannes. Lorsqu'un des liens du groupement tombe en panne, la capacité de transmission totale du groupement logique et du débit de l'ordonnanceur sont réduits de la même quantité. Le service prioritaire des files garantit que le trafic EF est toujours le premier à être servi en totalité, le trafic AF est second et selon la capacité résiduelle, BE est troisième. En cas de pannes, la proportion de trafic EF transmis sur les liens physiques restants devient plus grande qu'en cas de fonctionnement normal.

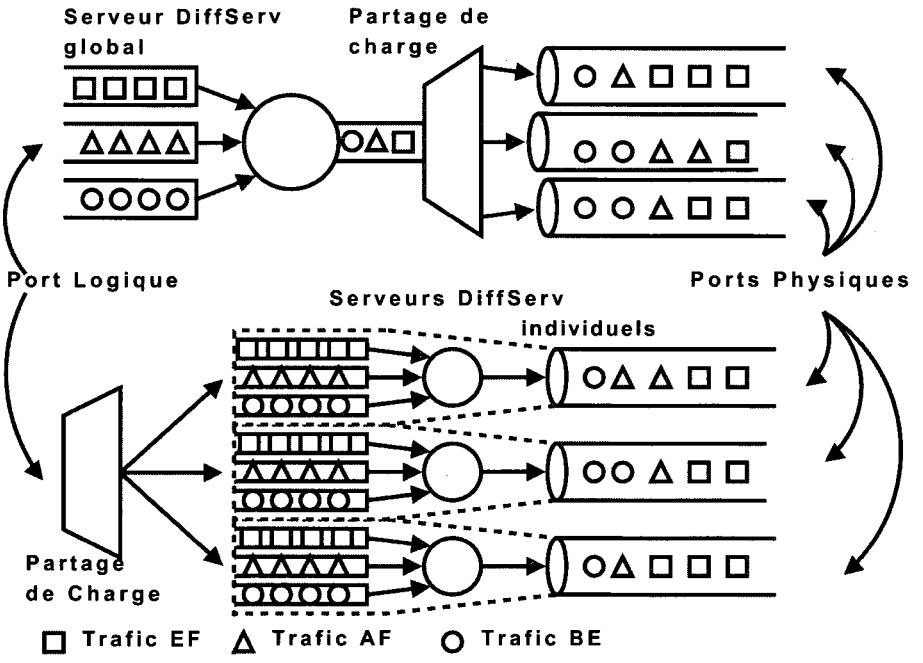


FIG. 5.4 Partage de charge avant et après la qualité de service

Étant donné qu'il n'est pas possible de réaliser le déploiement de DiffServ* comme le prévoit le modèle théorique, le bas de la figure 5.4 schématise l'implémentation de DiffServ* réalisée dans les commutateurs Atlas et Hercules. Nous pouvons voir dans ce cas que le partage de charge du trafic se fait *avant* l'application de la procédure de qualité service et cette dernière se fait sur chaque port physique du groupement de liens et non sur le port logique, i.e. l'Etherchannel au complet. *À priori*, il ne devrait exister en temps normal aucune différence majeure entre le modèle théorique et son implémentation puisque le trafic est, dans les deux cas, toujours servi de façon prioritaire par les mêmes canaux de transmissions physiques. Il existe cependant quelques différences essentielles quant à leur comportement en cas de pannes. Nous détaillons ces différences techniques dans ce qui suit.

5.2.2.1 Différenciation de service

Nous avons remarqué que seule une configuration minutieuses des mécanismes de différenciation de services donnera une allure DiffServ aux comportement des commutateurs. Bien qu'il soit possible de classifier le trafic suivant les DSCP, la différenciation de service ne se fait que par une configuration appropriée des politiques de surveillances, de marquage, de mise en file d'attente et d'ordonnancement de ces derniers. La configuration doit se faire en fonction de la quantité et composition du trafic et de l'effet désiré en cas de problèmes. Dans notre cas, nous voulons une protection absolue pour le trafic EF, un minimum de garanties pour le trafic AF et aucune protection particulière pour la classe BE.

Ceci étant dit, il existera certaines différences techniques entre le modèle DiffServ* théorique et son déploiement pratique. Dans le premier cas, la différenciation de service est configurée en fonction de la quantité de trafic et l'état du groupement de liens, ou Etherchannel dans ce cas, au complet. La quantité de trafic qui arrive au groupement de liens

est en moyenne constante et c'est la capacité de ce dernier qui varie en fonction de son état entièrement fonctionnel ou en cas de panne. Dans le deuxième cas, la différenciation de service est configurée en fonction de la quantité de trafic qui arrive à chaque lien du groupement et dépend alors de l'efficacité de l'algorithme de partage de charge et de l'état de chaque lien.

5.2.2.2 Taux de service maximal du trafic de haute priorité

L'ordonnancement prioritaire prévoit généralement une limite maximale sur le taux de service de la file d'attente la plus prioritaire. Ceci est nécessaire pour s'assurer que les classes de plus basses priorités reçoivent un service minimal. Si D_{EF} est la quantité maximale de trafic EF qui arrive à la file prioritaire, il serait alors envisageable de limiter le taux de service de cette file d'attente à $L_{EF} = D_{EF}$. Si la quantité de trafic EF dépasse cette limite, l'excédant est rejeté pour garantir que les autres classes de trafic aient une chance d'être servies.

C'est pourquoi il faut réserver un débit L_{EF} dans l'ordonnanceur du modèle DiffServ* théorique pour qu'une quantité D_{EF} soit toujours garantie un taux de service L_{EF} quelque soit l'état, fonctionnel ou en panne(s), de l'Etherchannel.

La pratique équivalente dans le cas de l'implémentation pratique de DiffServ* serait de réserver un taux maximal $L_{EF}/3$ pour une quantité $D_{EF}/3$ sur chacun des ordonnanceurs des trois ports physiques du groupement. Si un lien du groupement est en panne, un partage de charge équilibré mettra $D_{EF}/2 > L_{EF}/3$ sur chacun des liens fonctionnels restants. La protection EF ne sera pas optimale dans ce cas puisqu'un tiers du trafic de cette classe est rejeté. Le problème est partiellement réglé en limitant le taux de service EF sur chaque lien à $L_{EF}/2$. Ainsi, en cas de pannes, le trafic EF sera entièrement protégé sans toutefois pouvoir empêcher en temps normal la réduction de service des classes de plus

basses priorités aussi efficacement que dans le cas de DiffServ* théorique. Il est alors clair que la garantie de service dont doit bénéficier la classe EF est plus facilement réalisable avec la proposition théorique de DiffServ* qu'avec son implémentation pratique.

5.2.2.3 Ordonnancement prioritaire non offert

Nous choisissons l'ordonnancement prioritaire dans le modèle de DiffServ* théorique particulièrement pour sa capacité à garantir le meilleur taux de service et en conséquence une protection maximale au trafic prioritaire en cas de congestion. Cette méthode est idéale dans la mesure où il est possible de limiter la quantité de trafic prioritaire qui circule dans le réseau. Si cette quantité devient très importante, les flots de plus basses priorités risquent de ne recevoir aucun service.

L'alternative à l'ordonnancement prioritaire est le *Weighted Round Robin (WRR)* dans lequel chaque file d'attente est servie suivant un poids proportionnel à sa priorité, le service des flots prioritaires n'est pas absolu, mais WRR garantit toutefois un minimum de service aux files de basses priorités. La version Cisco du WRR est le *Shaped Round Robin (SRR)*. Quatre files d'attentes existent à chaque port physique de sortie et la méthode SRR permet d'attribuer un poids à chaque file d'attente qui ultimement définira la portion de la bande passante à laquelle le trafic de file en question aura accès. Par exemple si le poids des files est 12, 9, 6 et 3, l'allocation de bande passante à chaque file est respectivement $12/(12+9+6+3), 9/(12+9+6+3), 6/(12+9+6+3)$ et $3/(12+9+6+3)$ ou bien 40%, 30%, 20% et 10%. La file 1 se voit attribuer quatre fois plus de capacité que la file 4, la file 2 a trois fois la capacité de la file 4, etc... Le SRR peut fonctionner en deux modes, *shaped* ou *shared*. Dans le premier cas, l'allocation des pourcentages de capacité est rigide alors que le second permet un partage de la capacité allouée mais inutilisée d'une file avec les autres selon leur besoin.

Il faut aussi mentionner que les commutateurs 3750E de cette expérience permettent un ordonnancement hybride prioritaire-SRR dans lequel une des files a une priorité absolue sur les autres. Cette file est servie continuellement tant qu'elle n'est pas vide sans pour autant dépasser un taux maximal de service défini par un pourcentage spécifique de la capacité totale du lien du port en question. Les autres sont servies suivant les poids SRR qui leur sont attribués.

Pour cette étude, nous avions choisi la configuration hybride : une file prioritaire pour la classe EF et un service SRR pour les files des classes AF et BE. Le taux maximal de la file EF ainsi que les poids attribués aux files AF et BE ont été minutieusement choisis de façon à garantir une qualité de protection optimale en cas de panne au niveau de l'Etherchannel. La configuration technique des commutateurs Atlas et Hercules est expliquée dans l'annexe V.

5.2.2.4 Partage de charge équilibré

Un autre problème subsiste dans le partage de charge du trafic. Dans le cas de DiffServ* théorique, l'application des mesures de qualité de service est faite avant le partage de charge. Le débit de l'ordonnanceur étant toujours égal à la capacité totale du groupement de liens, qu'il soit fonctionnel ou en panne, il reste simplement à assurer un partage de charge équilibré du trafic sortant de l'ordonnanceur sur les différents ports de transmission physiques pour éviter tout rejet inutile de trafic.

Avec l'implémentation pratique de DiffServ*, non seulement faut-il partager le trafic de façon équilibrée sur les liens physiques fonctionnel, mais il faut aussi que le partage soit équilibré par classe. Il faut s'assurer que les mêmes proportions de trafic EF, AF et BE soient envoyés aux ordonnanceurs des ports physiques. Pour illustrer ce problème, considérons l'exemple de cette étude dans lequel le flot de données qui arrive à l'Etherchannel

est composé à parts égales de trafic EF, AF et BE. Un exemple de partage de charge valide et de mettre 100% du trafic EF sur le canal 1, 50%AF + 50%BE sur le canal 2 et le reste sur le canal 3. Ayant toute la demande EF sur un même port, la limitation de $L_{EF}/2 < D_{EF}$ causera une perte inutile de la moitié de ce trafic. Il faut ainsi s'assurer que le partage de charge soit équilibré en fonction du débit total de trafic et des débits particuliers des classes qui le composent.

La technologie Etherchannel est dotée d'un algorithme de partage de charge qui ne tient pas compte de la classe de service d'un flot de données mais seulement de l'adresse IP ou MAC de sa source et/ou de l'adresse IP ou MAC de sa destination. Étant donné que cette expérience est réalisée dans un espace contrôlé, il a été possible d'assurer un partage de charge équilibré par classe de service. Cette tâche peut être difficilement réalisable dans un environnement de réseau réel où les proportions de trafic changent dynamiquement. D'où un avantage clair de la méthode utilisée par le modèle théorique de DiffServ dans lequel le partage de charge se fait après l'application des procédures de qualité de service.

5.3 Performance et résultats en cas de pannes

Le trafic décrit à la section 5.2.1 a été généré et injecté dans le réseau de la figure 5.1. Tout le trafic généré par les machines 10 à 15 convergent vers l'Etherchannel pour atteindre leur destination suivant le schéma de la figure 5.5. Tout le trafic EF de VoIP et BE de données généré par les machines 10, 11, 12, 13, 14 et 15 a pour destinations respectives 17, 18, 19, 20, 15 et 16. Chaque machine source transmet deux vidéos simultanément, le premier suivant le même schéma de transmission que les flots EF et AF et, pour des simples raisons de diversité, la seconde transmission vidéo des machines sources suit le schéma du côté droit de la figure 5.5. La technologie de l'Etherchannel se base sur les adresses IP ou physiques sources et/ou destination pour effectuer le partage de charge. Pour nos tests, nous avons choisi l'option qui tient compte à la fois des adresses IP source et destination

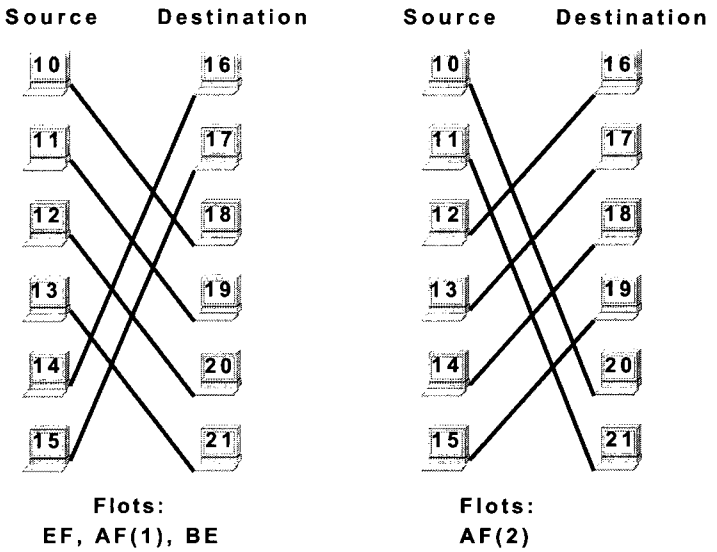


FIG. 5.5 Sources et Destinations des flots EF, AF, BE

pour assurer un partage de charge le plus diversifié possible. Pour chaque paire d'adresses possibles, l'Etherchannel calcule un nombre entre 0 et 7 et associe ce nombre avec un lien fonctionnel de l'Etherchannel. Ainsi, chaque flot est identifié par l'adresse IP de sa source et celle de sa destination et tous les paquets de ce flot sont envoyé sur le même lien composant de l'Etherchannel de façon à éviter tout problème de désordre de paquets suite au partage de charge. Tenant compte de nos configurations IP, seuls les schémas de transmission de la figure 5.5 ont permis un partage de charge équilibré du trafic quel que soit l'état de l'Etherchannel fonctionnel ou partiellement en panne.

Le tableau 5.2 donne plus de détails sur cette configuration. Nous pouvons voir qu'avec le premier et le second schéma de transmission, chacun des ports 22, 23 et 24 est utilisé exactement 2 fois dans le cas normal et, en cas de panne du premier lien branché au port 22 de l'Etherchannel, chacun des ports 23 et 24 restants est utilisé exactement par trois flots. Ceci montre que, conformément à la condition de partage équilibré de charge de la section 5.2.2.4, les flots demeurent répartis de façon équilibrée sur les ports fonctionnels de l'Etherchannel quel que soit son état. Étant donné que toutes les machines génèrent les mêmes demandes en trafic EF, AF et BE, nous avons un même débit de trafic EF, AF, BE

Schéma 1				Schéma 2			
Source	Destination	Normal	Panne	Source	Destination	Normal	Panne
10	18	22	24	10	20	22	23
11	19	23	23	11	21	24	24
12	20	24	23	12	16	22	24
13	21	23	24	13	17	23	23
14	16	24	24	14	18	23	24
15	17	22	22	15	19	24	23

TAB. 5.2 Allocation Flot/Port, cas normal ou avec panne du port 22

et total sur chacun des liens de l'Etherchannel. Cette dernière condition est essentielle au bon fonctionnement de la protection DiffServ*.

5.3.1 Résultats : EF-voix, AF-vidéo, BE-données

Un premier test de performance a été effectué avec la classification de base. Le trafic de voix, classifié EF, est le plus prioritaire et reçoit des garanties strictes de taux de perte, de délai bout-en-bout et de gigue. Le trafic de vidéo est considéré de moyenne priorité et est classifié AF. Le trafic de données appartient à la classe BE. Nous évaluons la qualité de protection du déploiement de DiffServ* en mesurant la débit de chacune des classes avant, pendant et après une période de panne aux diverses machines destination du réseau. La panne a été générée en débranchant physiquement un des câbles qui forment l'Etherchannel et ayant obtenu le même comportement aux six machines destinations, nous présentons aux figures 5.6 et 5.7 deux exemples de résultats.

Étant donné que le débit des classes EF et AF reste pratiquement constant quelle que soit la situation, ces figures nous permettent de conclure que la protection de ces flots est quasi-parfaite en cas de panne. Ceci constitue un résultat essentiel puisqu'à l'aide de DiffServ* seul nous avons réussi à protéger le trafic prioritaire de façon immédiate et totale. En raison de la grand variabilité du trafic AF, il n'est pas possible de conclure de

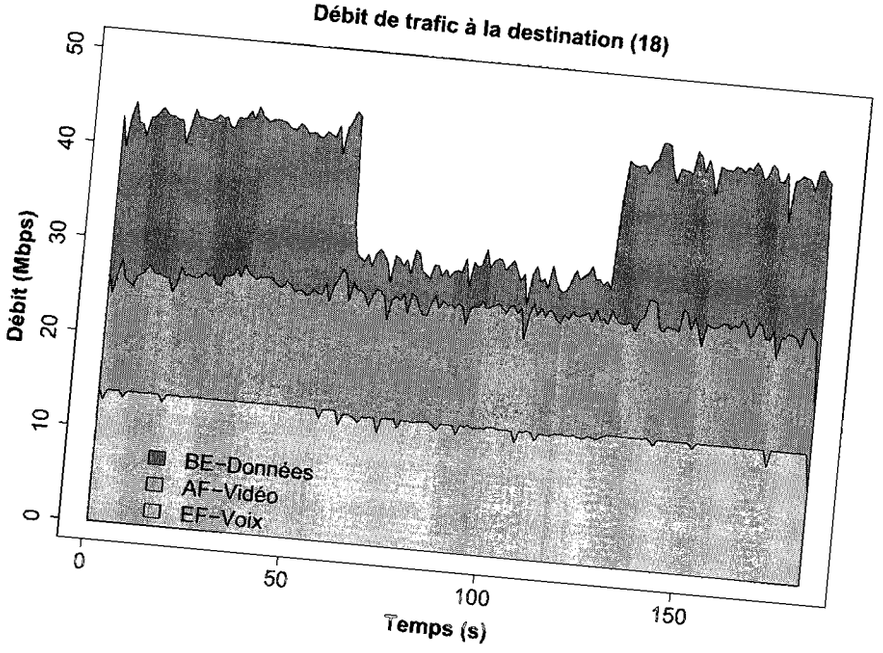


FIG. 5.6 Débit de trafic en cas de panne

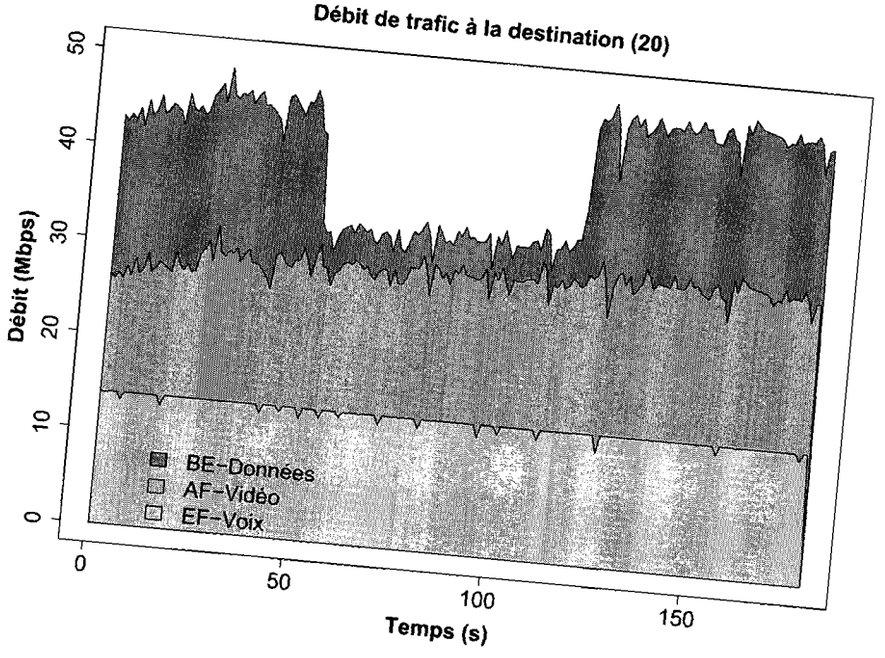


FIG. 5.7 Débit de trafic en cas de panne

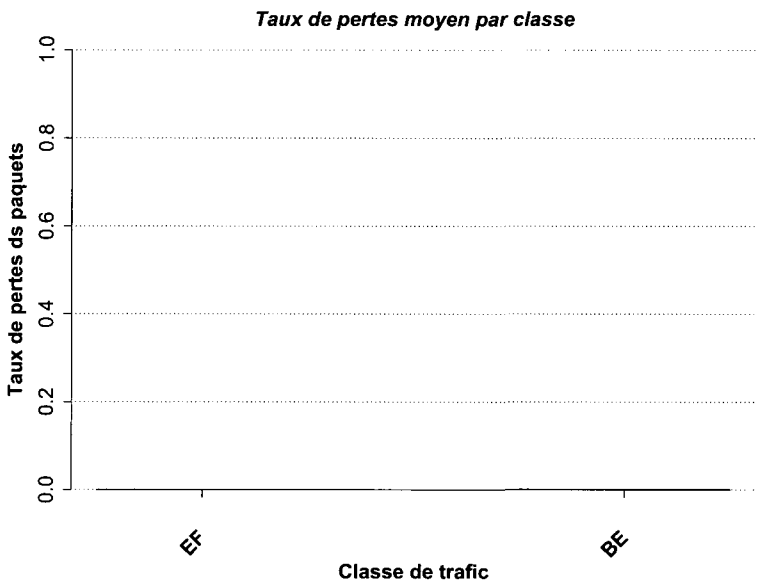
façon exacte sur la qualité de la protection offerte à cette classe en cas de pannes. Quant au trafic BE, il est clair que cette classe subit en grande partie les effets indésirables de la panne. Nous observons une diminution moyenne de 10 Mbps de trafic BE par machine et un total de 60 Mbps pour les six, une valeur proche de la quantité totale de trafic de 261.6 Mbps calculée précédemment moins la capacité de transmission de l'Etherchannel à deux liens de 200 Mbps.

Le logiciel D-ITG permet une évaluation quantitative de la qualité de service perçue par les flots qu'il génère. Ainsi, pour le trafic des classes EF et BE, nous avons pu évaluer la qualité de service en termes de taux de pertes, du délai bout-en-bout minimum, moyen et maximum et par deux mesures de variation du délai, l'écart type et la gigue. Les diverses mesures du délai sont évaluées grâce aux temps de génération des paquet à la machine source et de la date de leur réception à la machine destination. Pour avoir des mesures exactes, il faut calibrer les horloges de toutes les machines du réseau en utilisant le protocole *Network Time Protocol (NTP)* (Mills, 1992). Les résultats de taux de pertes, délai et gigue sont illustrés aux figures 5.8, 5.9 et 5.10.

Nous mesurons le taux de pertes des classe EF et BE en temps normal et sous l'effet d'une panne simple. Les figures 5.8(a) et 5.8(b) montrent qu' :

- en régime normal, aucune perte de paquets n'est observée, le réseau est bien dimensionné ;
- en cas de panne, la classe EF est effectivement immunisée contre tout rejet de paquets et que le système rejette près de 70% des paquets de la classe BE.

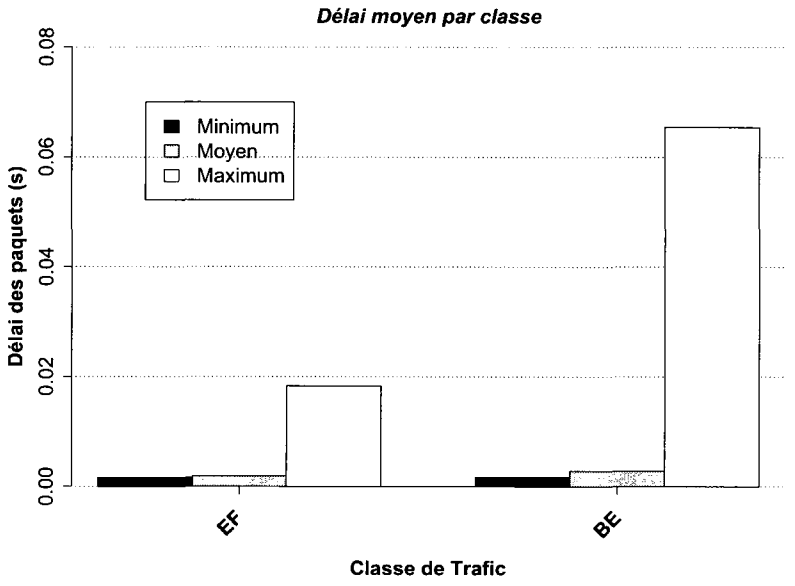
Des figures 5.9(a) et 5.9(b) nous pouvons voir que le délai minimum et moyen de la classe EF demeurent constants quel que soit l'état du système et nous observons une légère augmentation dans le délai maximum observé pour cette classe. Du côté BE, le délai moyen augmente de façon considérable, ce qui implique que des temps d'attentes plus longs pour les paquets non rejetés de cette classe.



(a) Cas normal

(b) Sous panne simple

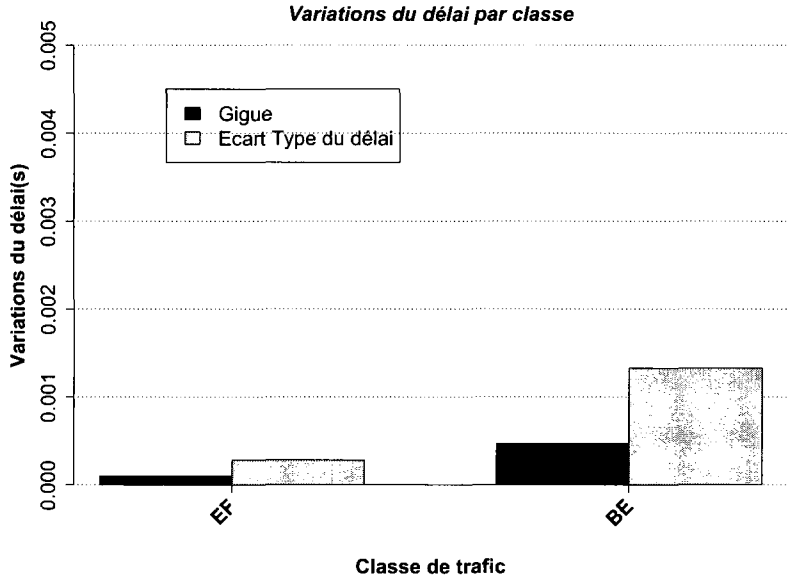
FIG. 5.8 Taux de pertes, EF et BE



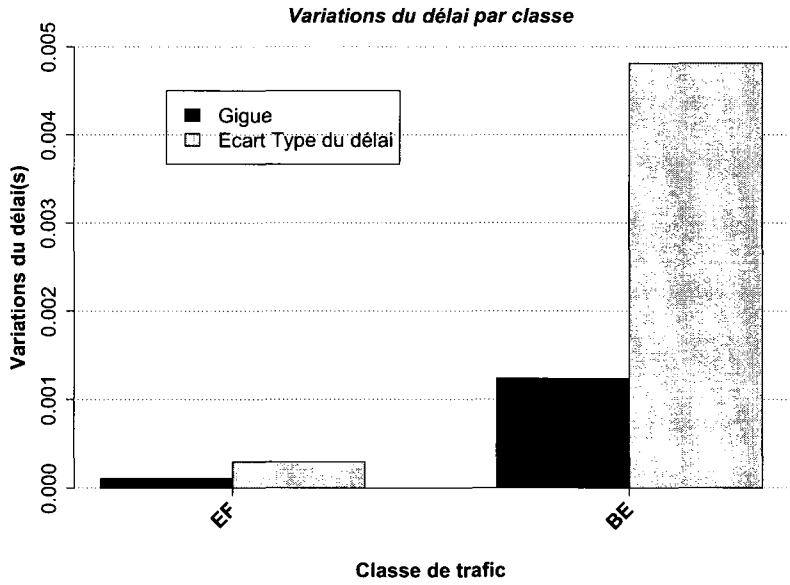
(a) Cas normal

(b) Sous panne simple

FIG. 5.9 Délai, EF et BE



(a) Cas normal



(b) Sous panne simple

FIG. 5.10 Gigue, EF et BE

En terme de variation du délai, les figures 5.10(a) et 5.10(b) montrent qu'en temps normal et sous pannes, le système conserve une gigue et un écart type de délai EF minimales. Les paquets BE sont encore les plus défavorisés et la gigue et l'écart type augmentent considérablement en cas de pannes.

Du point de vue d'un administrateur et concepteur de réseau, l'évaluation quantitative des mesures de qualité de service EF et BE permet de donner une indication claire sur la performance et essentielle à son amélioration. Cependant, il est aussi important d'évaluer la performance du réseau de façon qualitative du point de vue de l'usager. Nous prenons l'exemple de la qualité de service qualitative du trafic vidéo AF évaluée visuellement et montrée dans les figures 5.11 et 5.12. Bien que nous ayons établi précédemment (c.f. les figures 5.6 et 5.7), que le trafic vidéo semble être protégé de façon totale, ce résultat peut être acceptable pour un administrateur système mais l'est difficilement pour un usager.

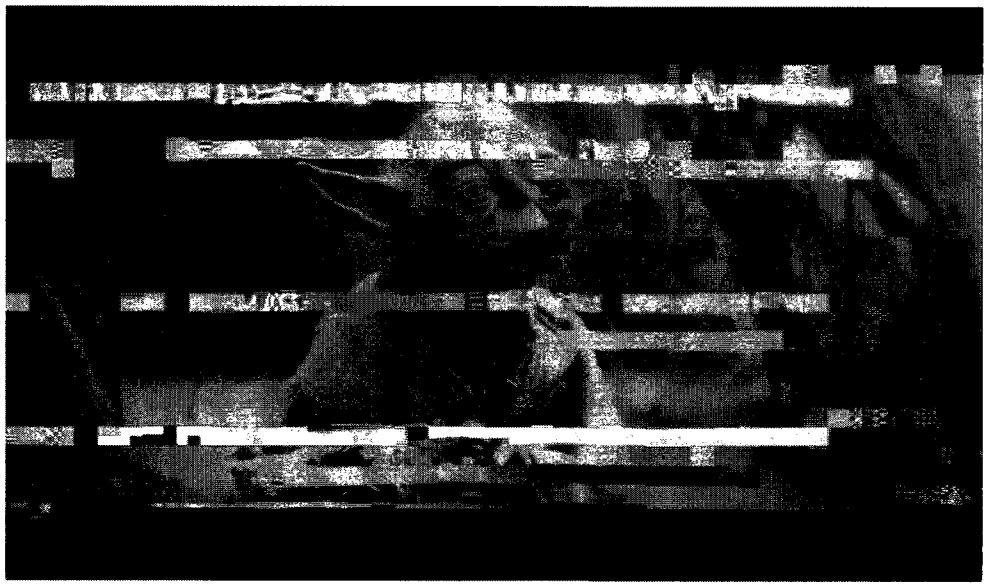


FIG. 5.11 Dégradation de performance vidéo visuelle, extrait de Starwars V

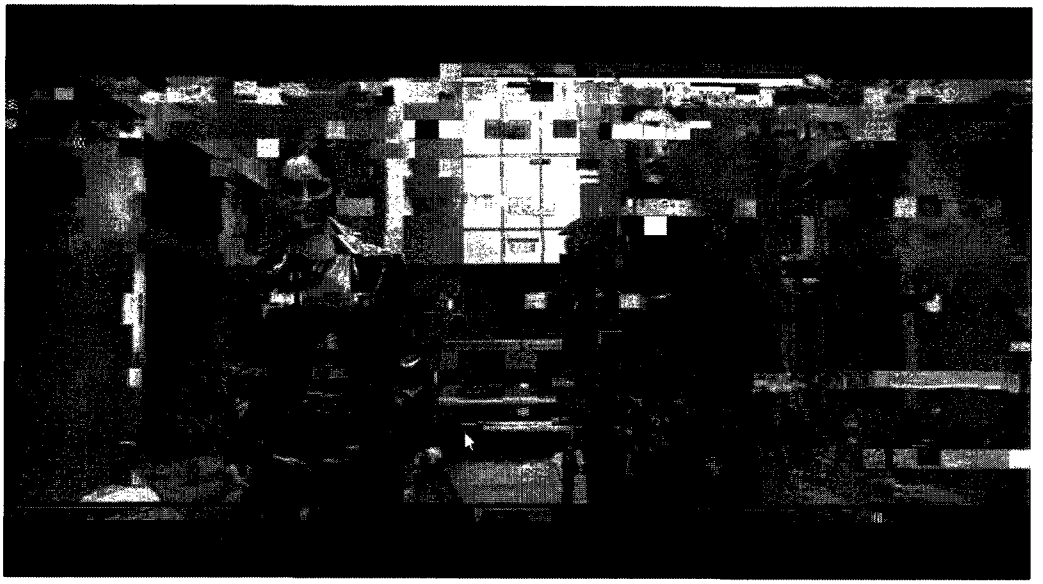


FIG. 5.12 Dégradation de performance vidéo visuelle, extrait de Matrix I

5.3.2 Résultats : EF-vidéo, AF-voix, BE-données

Nous avons présenté à la section 5.3.1 une analyse quantitative pour les classes EF et BE et seulement qualitative pour le trafic vidéo AF. Pour avoir une idée plus claire de la qualité de la protection offerte à cette dernière, nous menons ici la même étude que précédemment, à la seule différence que le trafic de vidéo est maintenant EF, la trafic de voix, généré et analysé par le logiciel D-ITG est AF.

Nous avons observé que, quel que soit la situation de l'Etherchannel, le trafic vidéo maintenant EF est protégé contre toute perte de paquets, tout délai excessif et toute dégradation visuelle et sonore de la qualité de la transmission à l'écran. Ceci confirme encore une fois que quel que soit la nature du trafic EF, DiffServ* lui offre une protection en cas de pannes.

Nous comparons le débit de trafic à certaines machines destinations, en régime normal à la figure 5.13 et en cas de panne aux figures 5.14 et 5.15. Nous pouvons voir qu'en cas de panne, le débit du trafic EF n'est pas affecté, celui du trafic AF de voix diminue légèrement et celui du trafic BE est grandement réduit. Une évaluation qualitative de la

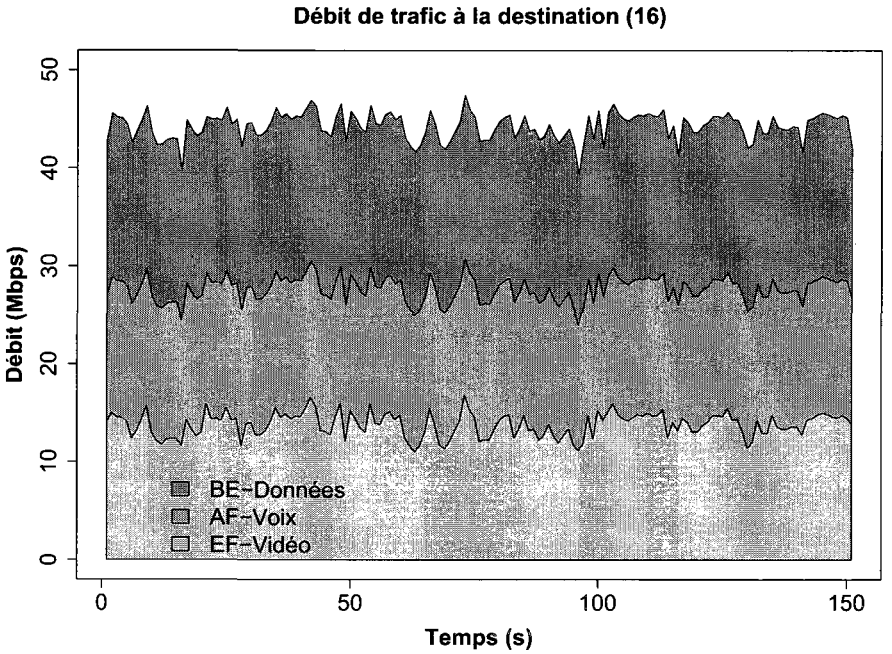


FIG. 5.13 Débit de trafic en temps normal (EF=vidéo)

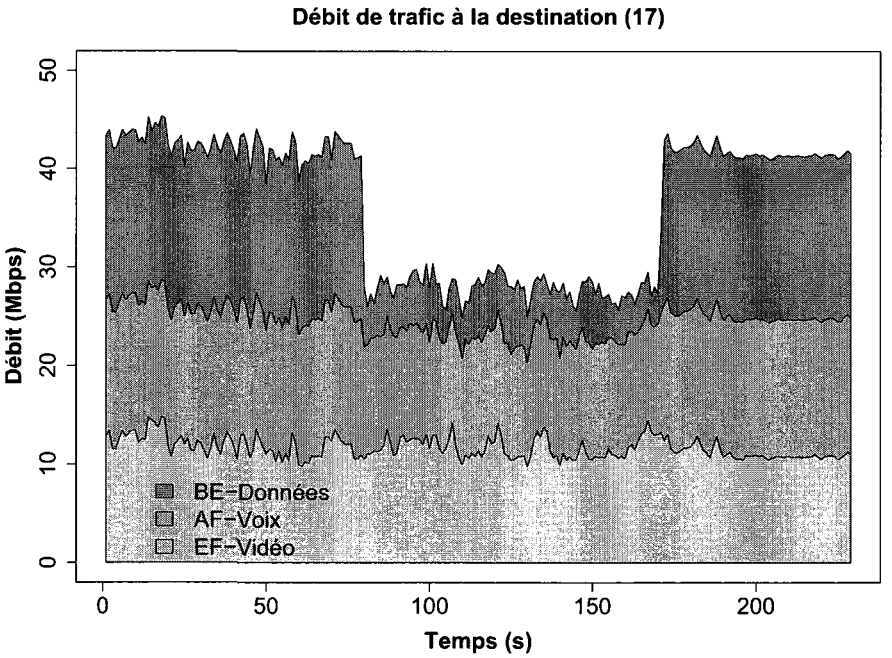


FIG. 5.14 Débit de trafic en cas de panne (EF=vidéo)

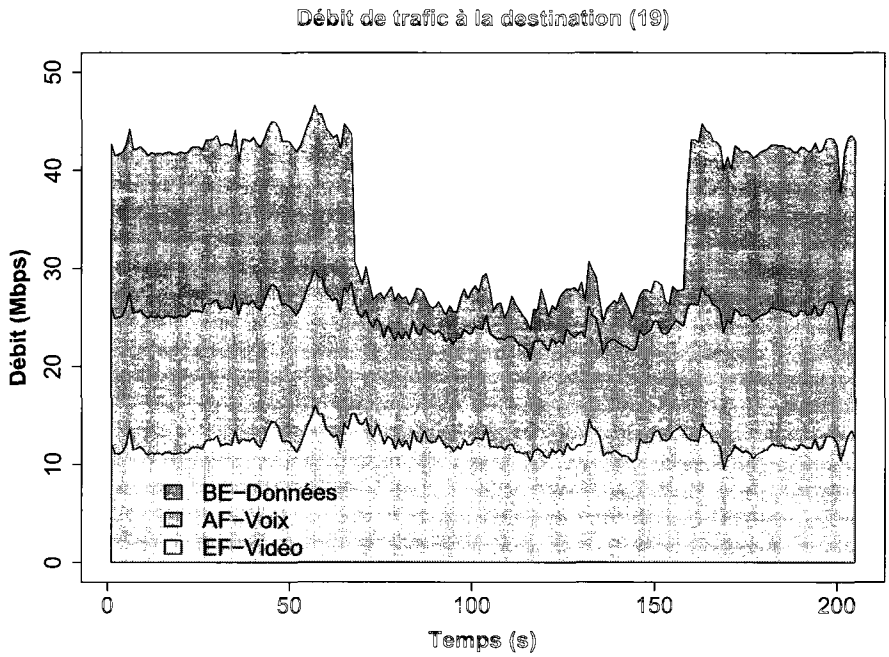


FIG. 5.15 Débit de trafic en cas de panne(EF=vidéo)

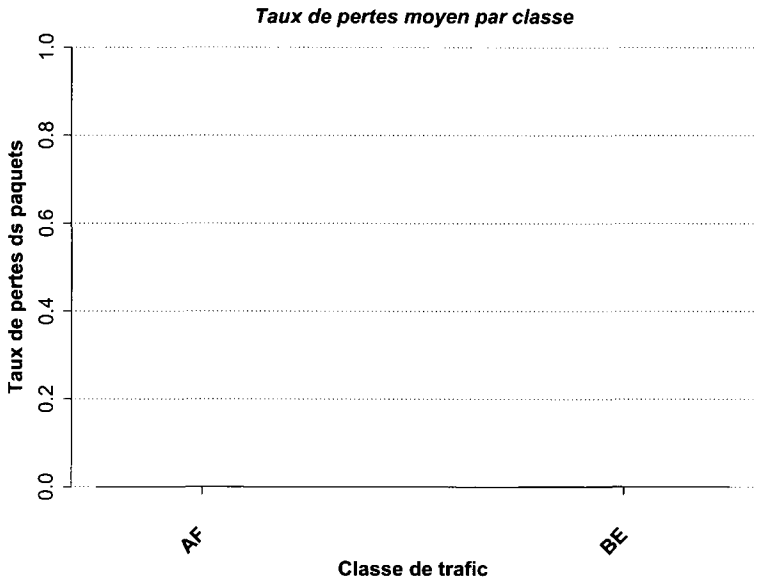
performance des classes AF et BE est montrée aux figures 5.16, 5.17 et 5.18.

Nous pouvons voir des figures 5.16(a) et 5.16(b) que le taux de pertes des paquets AF et BE est nul dans le cas normal et près de 5% pour la classe AF et dépasse 60% pour la classe BE. Ces résultats confirment encore nos résultats de la section précédente :

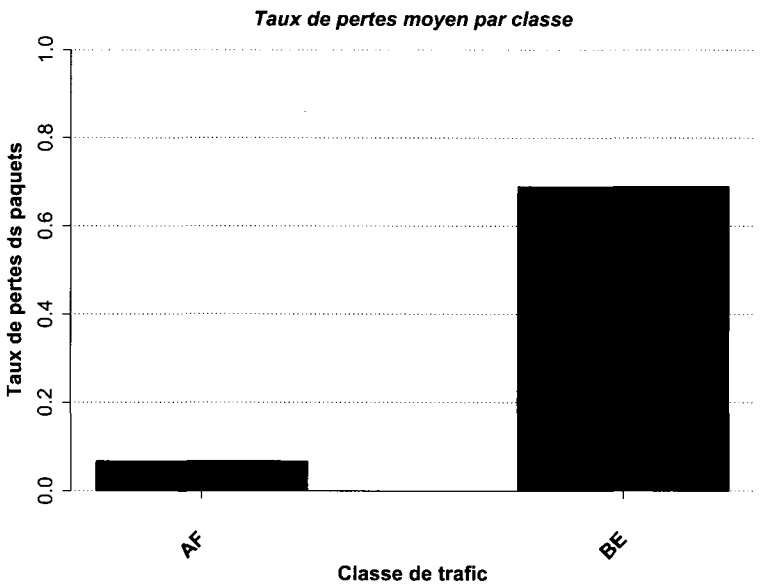
- la classe BE subit un taux de rejets considérables ;
- la qualité de protection de la classe AF est relativement proche de celle de la classe EF mais n'est pas idéale pour le trafic de transmission vidéo en temps réel.

Les figures 5.17(a) et 5.17(b) montrent que le délai moyen de la classe AF augmente légèrement alors que celui de la classe BE est largement supérieur en cas de panne. Encore une fois, la configuration des poids et de l'ordonnancement des files d'attentes assure un service rapide au paquets AF aux dépends des paquets BE qui sont mis en attente pour une durée plus longue en moyenne.

Les figures 5.18(a) et 5.18(b) montrent que la gigue et l'écart type du délai des paquets



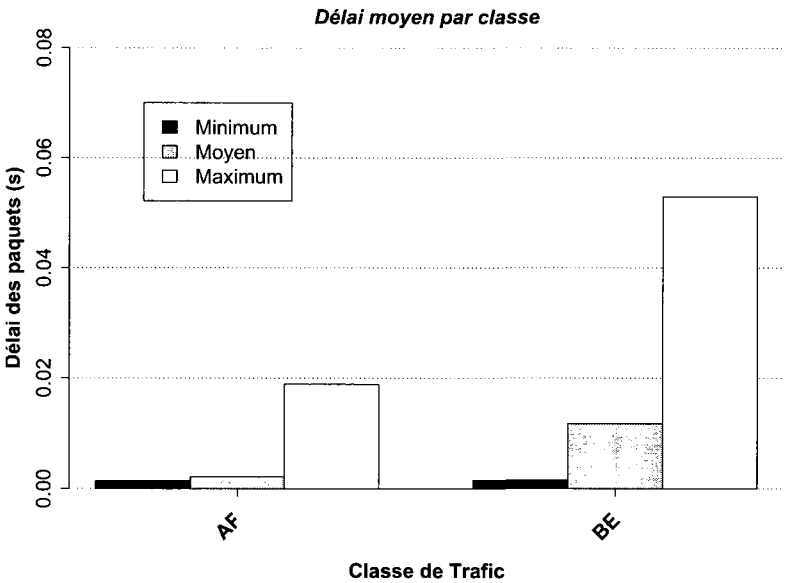
(a) Cas normal



(b) Sous panne simple

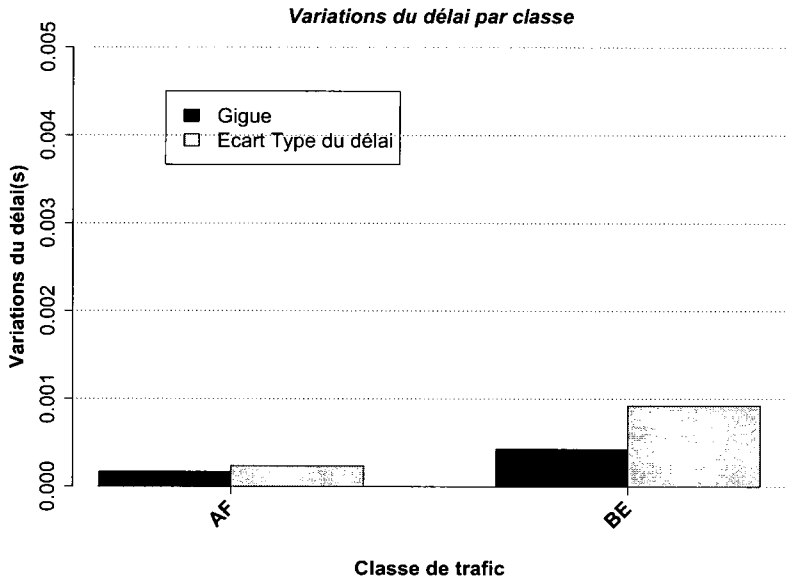
FIG. 5.16 Taux de pertes, AF et BE

(a) Cas normal

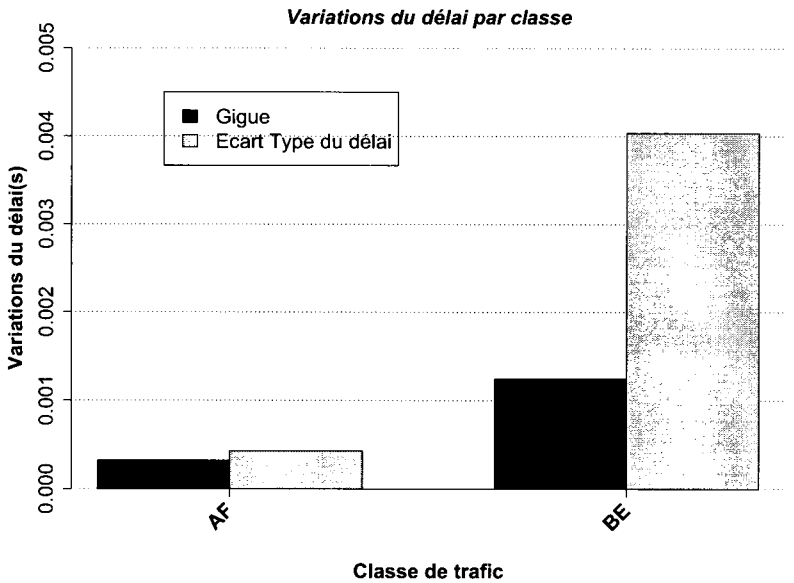


(b) Sous panne simple

FIG. 5.17 Délai, AF et BE



(a) Cas normal



(b) Sous panne simple

FIG. 5.18 Gigue, AF et BE

de la classe AF doublent en cas de panne. Ces mêmes valeurs pour la classe BE sont respectivement triple et quadruple.

Nous concluons de ces résultats que le classement des applications est très important et que la configuration des mesures de différenciation de service doit être faite en fonction des exigences particulières de chaque application. Un service vidéo impeccable n'a été obtenu qu'en utilisant la classe EF pour cette application. Il est possible de garantir un minimum de protection en cas de panne avec la classe AF mais ce dernier dépend grandement de la configuration du SRR et peut s'avérer inacceptable pour certaines applications.

5.4 Déploiement Etherchannel de DiffProtect

Cette étude démontre que les contraintes imposées par les équipements actuellement disponible n'empêchent pas le déploiement et le bon fonctionnement de la protection différenciée de DiffServ*. Nous avons aussi tenté de déployer DiffProtect à l'aide de la technologie de l'Etherchannel. Pour ce modèle de protection il faut :

- un partage de charge différencié par classe de trafic sur les différents liens d'un groupement ;
- une protection physique différente pour chacun de ces liens physiques.

Nous savons que la technologie Etherchannel ne permet aucun contrôle sur la façon dont le partage de charge est fait mais il est possible de déjouer cette limitation en configurant les machines pour générer du trafic unique. Nous aurons ainsi deux machines sources dédiées à la génération du trafic EF, deux autres à AF et les deux dernières aux flots BE. Avec un partage de charge qui se fait en fonction des adresses sources et destination, il est possible d'avoir tout le trafic EF sur un lien, le trafic AF sur un autre et BE sur le troisième, mais il n'existe toujours aucune garantie en cas de pannes. Si le lien Ethernet transportant le trafic de voix est débranché, rien ne garantit que ce trafic sera entièrement mis sur un quatrième câble fonctionnel. Il est de même pour la classe AF et particulièrement BE qu'on ne peut

empêcher le reroutage au sein de l'Etherchannel sur un câble fonctionnel.

Nous concluons alors que bien qu'il ait été possible de déjouer les limitations de la technologie Etherchannel pour assurer un déploiement pratique et fonctionnel de DiffServ*, cette tâche ne serait pas aussi évidente ni même possible pour DiffProtect. Ceci démontre la simplicité de DiffServ* en comparaison à DiffProtect ou tout autre mécanisme de protection différenciée physique. L'un ne requiert que la possibilité de combiner différenciation de services et groupement de liens alors que l'autre impose des exigences supplémentaires difficilement atteignables.

CHAPITRE 6

DIFFSERV* ET DIFFPROTECT : PLANIFICATION ET DÉPLOIEMENT

Nous avons vu au cours des chapitres précédents que le déploiement des deux modèles DiffServ* et DiffProtect se fait séparément pour chaque lien dans la couche logique et que tous deux utilisent une technique spéciale de routage et d'assignation de longueurs d'onde dans la couche de transmission optique inférieure. La grande différence entre les deux modèles provient de la méthode utilisée pour assurer une protection différenciée du trafic en cas de pannes simples et même multiples. DiffServ* se base sur l'architecture logique de différenciation de service de l'IETF pour assurer la protection du trafic contre les pannes de la couche inférieure. Le modèle DiffProtect combine l'utilisation de divers techniques de protection optique pour offrir un schéma de protection différenciée similaire à DiffServ*.

La performance des deux modèles a été sujette à plusieurs études et les résultats montrent que DiffServ* offre, en moyenne, un niveau de protection supérieur à celui de DiffProtect ; il est donc préférable de l'utiliser sur tous les liens IP du réseau. Les simulations ont aussi montré que dans certains cas de pannes extrêmes, et pour certains types de trafic, Diff-Protect offre une meilleure protection. Nous pouvons déduire que bien qu'il soit conseillé d'utiliser DiffServ* sur tous les liens du réseau, l'utilisation de DiffProtect peut être nécessaire à certains endroits où les pannes multiples sont plus fréquentes et les exigences en qualité de service et fiabilité sont plus strictes.

Le déploiement combiné de DiffServ* et de DiffProtect ne peut être réalisé de façon arbitraire et nécessite la résolution d'un problème d'optimisation multicouche qui apporte solutions aux problèmes essentiellement nouveaux :

- de déploiement de *deux* types de protection sur les liens de la couche logique ;
- de routage de flot *différencié* par classe de trafic en fonction de la protection dans la couche logique ;
- de routage de connexions optiques et d'assignation de longueurs d'ondes *par division* qui sépare les canaux d'un même lien logique et les place sur des chemins disjoints dans la couche physique.

Ce déploiement doit en même temps tenir compte :

- des caractéristiques de la topologie logique et de la topologie physique ;
- des exigences en qualité de service et du routage des différentes classes de trafic desservies par le réseau ;
- des contraintes topologiques de déploiement simultané de DiffServ* et DiffProtect ;
- des probabilité de pannes physiques et de la qualité de protection du réseau protégé par MixProtect.

Étant donné que la solution numérique ou mathématique d'un modèle d'optimisation de cette ampleur n'est généralement pas faisable, nous proposons à la section 6.1 une procédure à trois étapes complétée, à la section 6.2, par une modélisation mathématique qui réalise le déploiement de DiffServ* et de DiffProtect dans un environnement bicouche tel IP/WDM.

6.1 Procédure de déploiement de la protection MixProtect

La conception d'un réseau de communication multiservice est devenu synonyme de planification et de déploiement d'une procédure de protection différenciée du trafic capable :

- d'offrir un service préférentiel et adapté spécifiquement aux besoins en qualité de service de chaque application ;
- de garantir ce service quel que soit l'état, normal, en congestion ou sous panne(s), du

réseau.

Étant donné que la protection du trafic peut se faire aux niveaux physique et logique du réseau et qu'aucune méthode n'est sans inconvénients, le problème revient alors à déployer une protection *multi-niveau* qui combine le meilleur des deux couches réseaux.

MixProtect est une solution de protection à la fois différenciée et multi-niveau du trafic en cas de pannes physiques. Cette solution combine l'utilisation efficace et intelligente de DiffServ* et de DiffProtect pour garantir un optimum de protection quand la situation le requiert. Étant donnés les aspects innovateurs de DiffServ* et de son homologue DiffProtect, le déploiement de la solution MixProtect requiert l'élaboration d'une procédure de planification particulière.

6.1.1 Données du problème

La figure 6.1 illustre le point de départ de notre approche. Nous considérons que seules la topologie physique du réseau et la matrice de demande de trafic sont connues à cette étape. Nous justifions ce choix par le désir d'élaborer une approche de solution réaliste, applicable à tout réseau optique actuel où une topologie fixe et une matrice de trafic connue sont généralement des conditions préexistantes.

La topologie physique détermine l'emplacement des noeuds du réseau et des liens qui les relient et chaque lien physique est une fibre optique sur laquelle le multiplexage de longueurs d'onde est possible grâce à la technologie WDM. La matrice de trafic indique le volume de trafic qui doit être acheminé d'une source vers une destination du réseau logique.

L'objectif est ainsi de dimensionner la topologie logique en déterminant l'emplacement, la capacité, la quantité de trafic et la protection de chacun de ses liens logiques. Pour atteindre cet objectif, nous proposons une procédure à trois étapes :

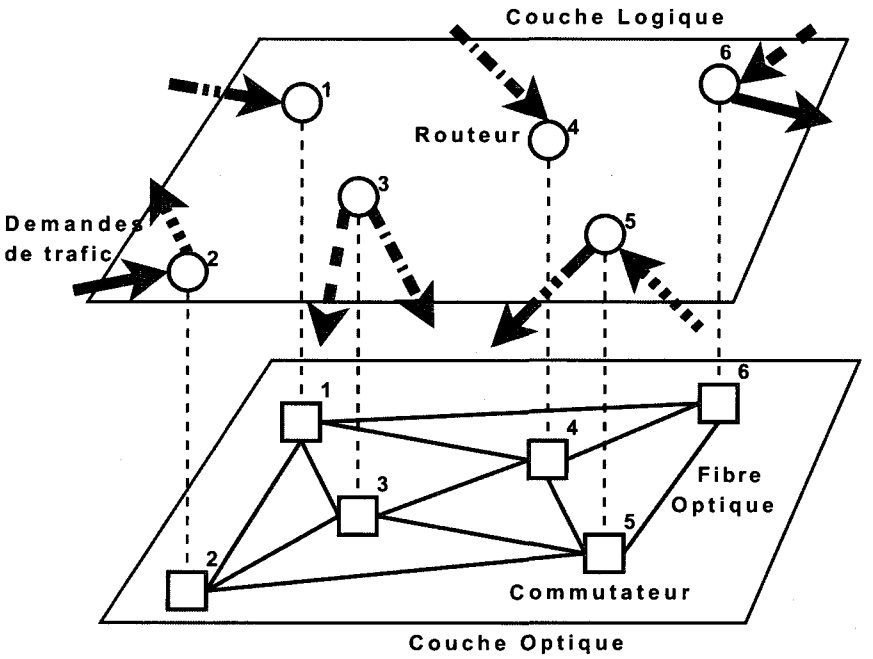


FIG. 6.1 Initialisation : Demandes de trafic logique et topologie physique

– le dimensionnement de la couche logique et déploiement de DiffServ* ;
– l'analyse de fiabilité et déploiement de DiffProtect ;
– le routage de flot différencié dans la couche logique protégée par MixProtect.

Chacune de ces étapes permet de réaliser une partie des objectifs et l'ensemble doit être appliqué dans un ordre donné. Le concepteur garde l'option d'arrêter à la fin d'une étape quelconque si toutes ses exigences sont satisfaites.

6.1.2 Dimensionnement DiffServ* de la topologie logique

Cette étape a pour but de construire une topologie logique qui permettrait l'acheminement de la totalité de la demande de trafic entre les différentes sources et leurs destinations respectives du réseau. Une des variables de décision principales est la détermination de l'emplacement des différents liens logiques. Chaque lien logique correspond à une demande d'une ou plusieurs connexions optique entre les noeuds physiques correspondants.

Chaque connexion est établie à l'aide d'un canal optique qui est assigné à une longueur d'onde particulière le long d'un chemin physique choisi. La capacité d'un lien logique est égale à la capacité ou la somme des capacités du ou des canaux optiques qui lui sont réservés. Le choix des liens logiques, le routage du trafic au niveau logique, l'assignation des longueurs d'onde et le routage des canaux optiques dans la couche physique doivent se faire sous les contraintes de DiffServ* et avec objectif de minimiser la quantité de ressources de transmission physiques nécessaire au déploiement.

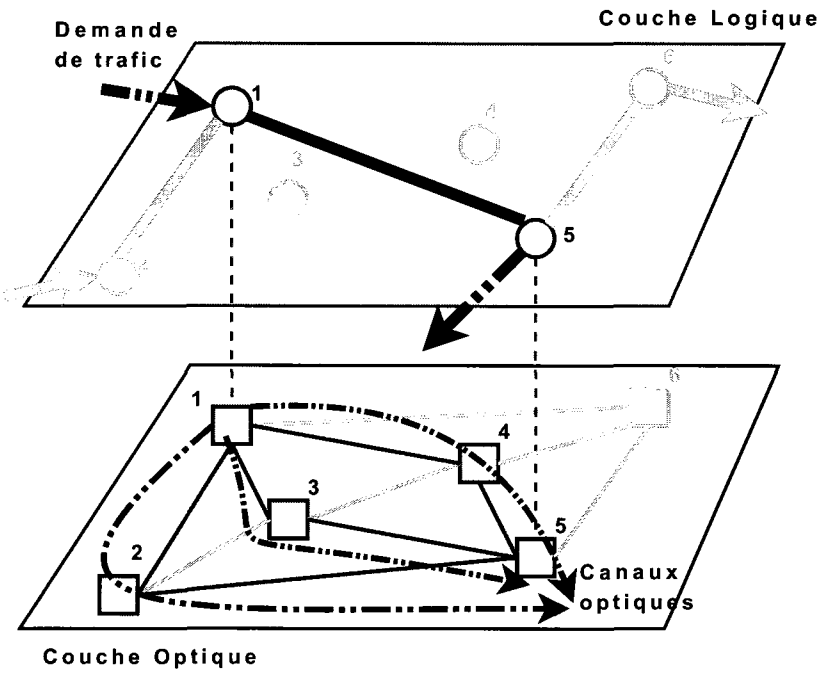


FIG. 6.2 Étape 1 : Déploiement de DiffServ*, dimensionnement et routage logique

La figure 6.2 illustre l'exemple du lien logique $(1, 5)$ dont la mise en place serait souhaitable pour satisfaire la demande de trafic entre ces deux noeuds. La protection DiffServ* du lien logique $(1, 5)$ impose certaines contraintes sur le nombre de canaux optiques mis en place pour chaque lien ainsi que sur le routage de ces derniers sur la topologie physique. Il faut au minimum *trois* canaux optiques par lien logique mis en place, dans la mesure du possible, sur trois chemins *physiquement disjoints*. Ces contraintes ont pour conséquence directe que les liens logiques ont tous *la même* capacité égale à la somme de celle de trois

canaux optiques mais qui sont évidemment *plus robustes* face aux pannes physiques. En effet, l'exemple de la figure 6.2 montre une application directe de ces contraintes :

- les trois canaux optiques du lien logique $(1, 5)$ mis en place sur les chemins physiques disjoints $[1, 3, 5]$, $[1, 2, 5]$ et $[1, 4, 5]$;
- la panne de tout sous-ensemble de ces chemins cause au plus une diminution de capacité de $(1, 5)$ et permet à DiffServ* de protéger le trafic prioritaire sur ce lien.

6.1.3 Déploiement de DiffProtect et protection multi-niveau

Nous obtenons à la fin de l'étape 1 une topologie bicouche complète dans laquelle le trafic de la couche logique est entièrement protégé par DiffServ*. Si le concepteur du réseau juge la qualité de cette protection satisfaisante, il pourrait arrêter à ce stade ou encore continuer avec le déploiement de DiffProtect là où la situation l'exige. Cette tâche est facilitée par le fait que les pré-requis topologique de DiffServ* sont également valables pour DiffProtect. Les deux modèles exigent trois canaux optiques disjoints pour la transmission du trafic mais DiffProtect requiert *en plus* des canaux de protection.

Il a déjà été établi que le déploiement de DiffProtect et de DiffServ* doit être accompli en se basant sur les exigences en qualité de protection de certaines classes de trafic. Bien que nécessaire, cette règle demeure en principe insuffisante étant donné la nature de l'expérience par simulation réalisée. Nous avons voulu une évaluation juste et équitable de la qualité de protection des deux modèles pour aboutir à des conclusions générales qui ne dépendent d'aucune contrainte ou configuration topologiques de réseaux physiques particulières. Nous avons dissocié l'évaluation de la qualité de protection des deux modèles des variables topologiques en considérant une abondance de ressources physiques qui assurerait un déploiement idéal des deux mécanismes de protection quelle que que soit la localité ainsi qu'une équiprobabilité et une indépendance entre les pannes des ca-

naux optiques. Étant donné que ces suppositions reflètent rarement la réalité des réseaux actuels, il est alors nécessaire de tenir compte des contraintes topologiques dans le choix de positionnement de DiffProtect dans le réseau.

Une première tient compte des exigences topologiques de DiffProtect. En plus des trois canaux principaux qui forment un lien logique protégés par DiffServ*, DiffProtect requiert la mise en place de deux canaux de supplémentaires, l'un dédiée à la protection du trafic de haute priorité du seul lien en question, l'autre à une protection du trafic de moyenne priorité d'un ou plusieurs autres liens logiques. Pour un maximum de performance, ces canaux de protection doivent être disjoints des trois premiers. Ceci impose une première contrainte topologique caractérisée par la nécessité de trouver un minimum de quatre chemins physiquement disjoints pour le routage des canaux optiques d'un lien logique protégé par DiffProtect.

Une deuxième contrainte vient du fait que nous utiliserons DiffProtect selon la probabilité des pannes simples et multiples qui peuvent affecter les canaux optiques d'un lien logique particulier. Nous savons déjà que DiffProtect est plus avantageux que DiffServ* seulement dans certaines situations de pannes multiples et pour certaines classes de trafics particulières. Nous aurons donc intérêt à tenir compte des probabilités des pannes multiples au sein des différents liens logiques dans le positionnement de la protection DiffProtect dans le réseau.

La deuxième étape de cette procédure se base essentiellement sur ces deux contraintes pour déployer DiffProtect. Il s'agit en premier lieu de spécifier les positions de DiffProtect par ordre de :

- nécessité quand la probabilité de panne est inacceptable ;
- possibilité quand la topologie physique le permet.

Une fois accomplie, la mise en place de DiffProtect sur certains liens logiques doit se faire

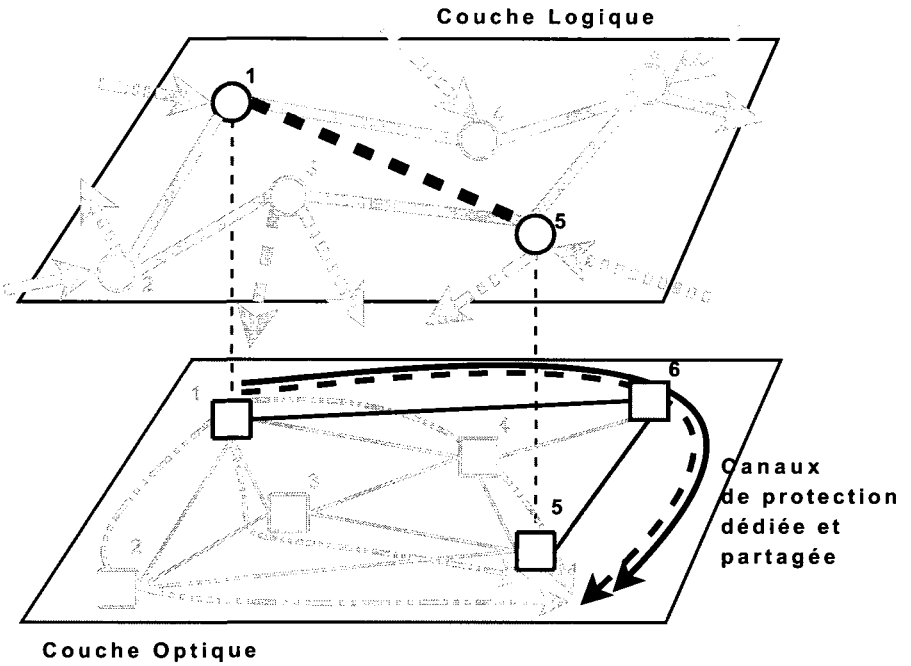


FIG. 6.3 Étape2 : Probabilité de panne et déploiement de DiffProtect

en minimisant la quantité de ressources allouées à la protection physique du trafic en cas de pannes.

La figure 6.3 illustre les réalisations de cette étape. La topologie logique demeure inchangée tout au long de cette étape et des modifications sont apportées à la seule topologie physique selon la méthode de protection requise. Nous reprenons l'exemple du lien logique $(1, 5)$ préalablement protégé par DiffServ*. Ce lien est formé par trois canaux optiques mis en place sur les chemins physiques $[1, 2, 5]$, $[1, 3, 5]$ et $[1, 4, 5]$. En connaissant la probabilité de panne de chaque lien physique, il est possible d'évaluer la probabilité qu'une panne simple, double ou triple affecte le lien logique. Si P_{ij} est la probabilité que le lien physique $[i, j]$ soit en panne et en supposant que les pannes de liens et de chemins sont indépendants nous aurons :

– Probabilité P_a, P_b et P_c que les chemin $[1,2,5]$ à $[1,4,5]$ soient en panne :

$$P_a = 1 - (1 - P_{12})(1 - P_{25}) \tag{6.1}$$

$$P_b = 1 - (1 - P_{13})(1 - P_{35}) \tag{6.2}$$

$$P_c = 1 - (1 - P_{14})(1 - P_{45}) \tag{6.3}$$

– Probabilité P_F d'aucune panne dans le lien logique $(1,5)$ donc 100% fonctionnel :

$$P_F = (1 - P_a)(1 - P_b)(1 - P_c) \tag{6.4}$$

– Probabilité P_S d'une panne simple d'exactement 1 canal dans le lien logique $(1,5)$

$$P_S = P_a(1 - P_b)(1 - P_c) + P_b(1 - P_a)(1 - P_c) + P_c(1 - P_a)(1 - P_b) \tag{6.5}$$

– Probabilité P_D d'une panne double d'exactement 2 canaux dans le lien logique $(1,5)$

$$P_D = P_aP_b(1 - P_c) + P_aP_c(1 - P_b) + P_bP_c(1 - P_a) \tag{6.6}$$

– Probabilité P_T d'une panne triple d'exactement 3 canaux dans le lien logique $(1,5)$

$$P_T = P_aP_bP_c \tag{6.7}$$

Si le concepteur de réseau juge que la probabilité P_D est inacceptable, DiffProtect devient alors nécessaire sur le lien logique $(1,5)$. Étant donné la disponibilité d'un quatrième chemin physique disjoint des trois premiers entre les noeuds 1 et 5, le déploiement de DiffProtect dans sa forme *la plus robuste* est aussi possible. La figure 6.3 illustre ce déploiement où les deux canaux de protection sont mis en place sur le chemin $[1,6,5]$ disjoints des trois premiers.

6.1.3.1 Protection multi-niveau lien par lien

L'application de l'approche décrite à l'étape 2 résulte en un réseau doté d'une protection différenciée et *multi-niveau* assurée dans la couche logique par DiffServ* et dans la couche physique par DiffProtect. Il faut noter que DiffServ* et DiffProtect sont tous deux des modèles de protection de type *lien par lien*. Les liens logiques sont donc munis de l'une *ou* l'autre des techniques de protection résultant en une partie du réseau protégée par DiffServ* et une autre par DiffProtect.

Dans cette optique, notre solution de protection MixProtect est à la fois non conventionnelle et innovatrice puisqu'en général, la protection mutli-niveau, au sens traditionnel du terme, implique l'élaboration de deux politiques de protection, l'une, physique, déployée sur l'ensemble du réseau physique, l'autre, logique, déployée sur l'ensemble de la topologie logique. Ainsi, la protection multiniveau peut se faire :

- de façon séquentielle, premièrement dans la couche physique et comme deuxième recours dans la couche supérieure ;
- suivant une procédure de coordination et de collaboration, parfois complexe, dans laquelle la situation est analysée en but de décider sur le partage de la tâche de protection entre les couches.

D'un côté, nous proposons DiffServ*, un modèle de protection logique rapide, performant et fiable, qui permet d'éviter la nécessité de passer en premier lieu par la protection physique. D'un autre, un flot circulant sur un chemin logique particulier est à certains endroits protégé par DiffServ*, à d'autres DiffProtect. Il s'en suit alors que la protection reste alors multi-niveau mais *par partie* puisqu'elle permet d'éliminer toute nécessité de coordination de la protection entre les deux couches.

6.1.3.2 Routage du trafic en fonction de la protection

Nous invoquons à l'étape 2, la *nécessité probabiliste* et la *possibilité topologique* comme seuls critères lors du processus de déploiement de DiffProtect. Nous ne tenons pas compte *pour l'instant* du routage dans la couche logique et des exigences en qualité de service des flots des différentes classes. Ceci est en effet une conséquence directe de la nature du problème à résoudre. La préexistence d'une topologie physique fixe introduit des contraintes de déploiement incontournables et plus fortes à ce stade que les critères de qualité de service de quelques flots particuliers. Ainsi, après un routage préliminaire des flots à l'étape 1 et le déploiement de DiffProtect à l'étape 2, une troisième étape est nécessaire pour raffiner le routage initial dans le but d'optimiser la protection MixProtect en fonction des besoins et caractéristiques de chaque classe de service du réseau. Le routage est alors réévalué en fonction de la protection et non l'inverse.

6.1.4 Différencier le routage pour maximiser la protection

Nous illustrons à la figure 6.4 un exemple du résultat complet de la phase 2 de notre procédure de solution. Nous pouvons voir que DiffServ* est utilisé sur un sous-ensemble des liens de la couche logique et DiffProtect sur le sous-ensemble complémentaire. Nous allons spécifier ultérieurement qu'une réévaluation du routage des flots dans la couche logique est nécessaire et doit être réalisée en fonction des nouvelles données de protection. Étant donné l'existence de plusieurs classes de trafic avec des exigences variées de niveau de protection, il serait souhaitable de mettre en oeuvre un processus de *routage différencié* qui dépende à la fois de la qualité de service requise par un flot et de la combinaison de protection appliquée sur le chemin logique qu'il utilise.

Il est à noter que nous ne savons pas calculer une relation mathématique exacte et directe entre les probabilités de panne sur un chemin, la combinaison de protection utilisée

et la qualité de service subséquente des classes de flots qui parcourent ce chemin. Nous proposons alors d'utiliser une *méthode par pénalité* basée sur les résultats de l'étude par simulations pour déterminer un routage optimal des différents flots du réseau. Pour chaque paire origine/destination de trafic et pour chaque chemin logique qui les relie, nous évaluons deux paramètres de pénalités :

- le premier dépend du nombre de liens protégés d'un chemin par DiffProtect ;
- le second dépend de la position relative des liens DiffProtect sur le chemin.

Une pénalité élevée indique que ce chemin est défavorable pour une classe de flot particulier et il serait souhaitable de réduire au maximum la quantité de trafic de cette classe préalablement routé sur ce chemin.

Si nous revenons à la figure 6.4, toute la demande de trafic entre les noeuds 2 et 6 a initialement été routée sur le chemin logique $(2, 1, 5, 6)$. Après le déploiement de DiffProtect et comme détaillé à la section 6.2.3.1, il est possible d'évaluer les paramètres de pénalité de chacun des chemins $(2, 1, 5, 6)$, $(2, 3, 5, 6)$ et $(2, 1, 4, 6)$. À l'aide de cette information, il devient alors possible de détourner certains flots, notamment AF dans ce cas, du chemin choisi à l'étape 1 sur le chemin $(2, 1, 4, 6)$ évalué comme étant plus favorable à l'étape 3. La procédure de détournement et conséquemment de routage différencié du trafic est appliquée à tous les flots. Elle est sujette aux contraintes de capacité des différents liens de la couche logique et vise à minimiser la pénalité globale du routage versus la protection du réseau entier. Il est nécessaire de mentionner que cette étape d'optimisation concerne uniquement la couche logique et qu'aucune modification n'est apportée à la structure de la topologie physique. Un avantage clair de cette approche est la possibilité de pouvoir réorganiser le routage en fonction d'une matrice de demande de trafic qui change dynamiquement sans avoir besoin de modifier la structure du réseau sousjacent.

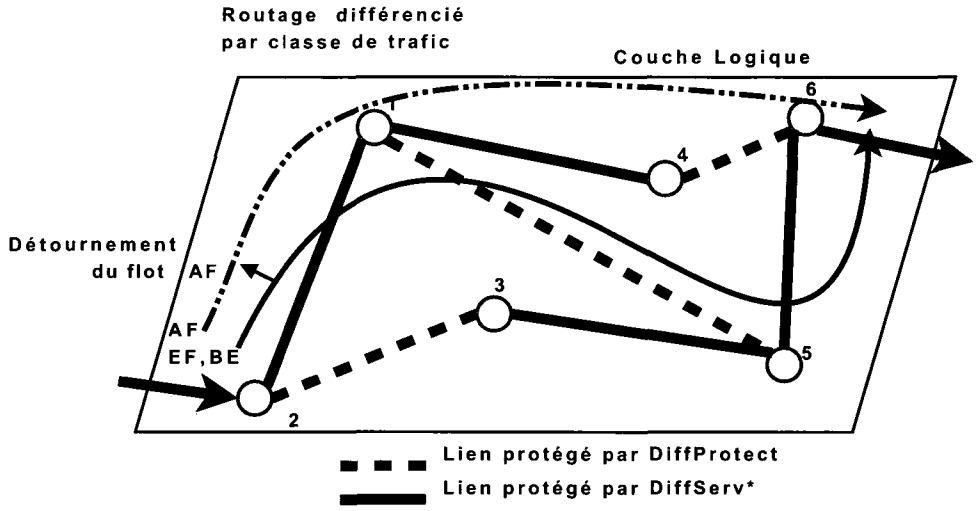


FIG. 6.4 Étape3 : Pénalité de protection, routage différencié et détournement de flots

6.2 Modélisation mathématique

La modélisation mathématique de notre solution à trois étapes est décrite dans cette section. La première partie est détaillée à la section 6.2.1. Elle montre un modèle qui déploie DiffServ* sur tous les liens du réseau tout en minimisant la quantité de ressources optiques nécessaire. Après avoir identifié les liens du réseau logique les plus sensibles aux pannes multiples, la protection de ces liens doit être changée pour DiffProtect. La deuxième partie du modèle est décrite dans la section 6.2.2, elle réalise le déploiement de DiffProtect où il est exigé et le fait tout en minimisant la quantité de ressources optiques nécessaire. Finalement, la section 6.2.3 de ce chapitre utilise une technique de reroutage et détournement de flot pour optimiser la performance du réseau en fonction de la combinaison MixProtect choisie.

6.2.1 Modèle 1 : Déploiement de DiffServ*

Le déploiement du modèle de protection DiffServ* sur un lien (i, j) d'un réseau IP n'est possible que quand ce lien est un regroupement d'au moins trois chemins optiques établis entre les routeurs i et j. Le modèle mathématique de cette section est inspiré de (Sivalingam and Subramaniam, 2000) et est ensuite modifié pour accommoder les contraintes supplémentaires de DiffServ*. Étant donné une topologie optique connue ainsi qu'une matrice de demande de trafic IP, le modèle à pour objectif 1) de définir la topologie IP correspondante, 2) router la demande de trafic IP sur cette topologie, 3) d'assigner ω chemins optiques à chaque lien IP et finalement 4) de router ces chemins optiques sur le maximum de routes physiquement disjointes possible. La capacité des liens IP est fixe et égale à la somme des capacités des ω chemins optiques qui lui sont associés.

6.2.1.1 Variables et paramètres du modèle

Nous montrons dans la figure 6.5 un réseau IP/WDM à deux couches. Au niveau de la couche physique nous avons un topologie en maille avec N_p noeuds et plusieurs liens de fibre optique qui les relient. En correspondance avec la couche optique, on ne voit que N_l noeuds logiques, ou routeurs, dans la couche IP. Étant donné une matrice de demande de trafic entre les différentes paires de noeuds o et d logiques, le programme complète la topologie logique en choisissant la position de ses liens et décide de la quantité de trafic que ces liens doivent transporter de façon à respecter la demande. Pour la topologie physique, le programme doit utiliser certaines longueurs d'onde d'une série de liens physiques $[l, m]$ pour mettre en place ω canaux optiques pour chaque lien logique. Pour garantir la protection DiffServ*, les canaux optiques doivent être mis en place sur des chemins physiquement disjoints. En référence à la figure 6.5, si nous devons mettre en place un lien logique entre les noeuds logiques i et j alors les chemins en pointillé de la couche physique montrent quels liens physiques les ω chemins optiques qui relient i à j

peuvent utiliser. Avec l'architecture DiffServ* sur le lien logique (i, j), les flots prioritaires qui circulent sur ce lien sont toujours protégés contre une ou plusieurs pannes qui peuvent survenir sur un ou plusieurs des canaux optiques qui forment les liens logiques qu'ils traversent.

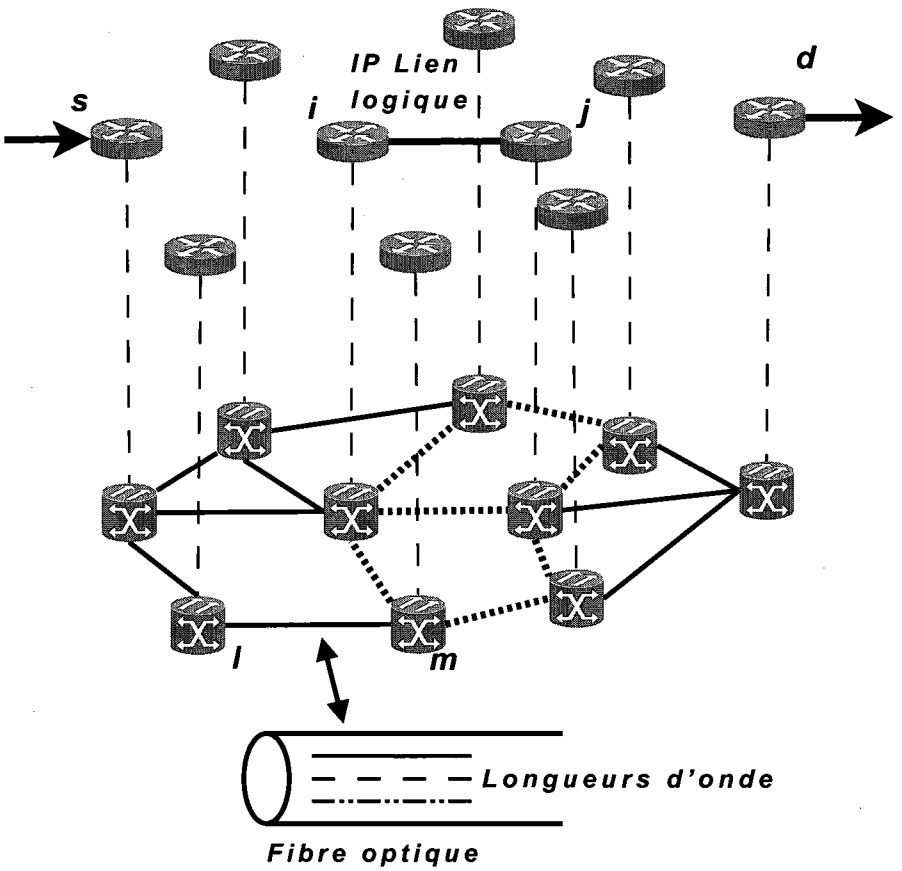


FIG. 6.5 Un réseau IP/WDM à deux couches

Les paramètres et données

- ω est le nombre de chemins optiques réservés à chaque lien logique. Dans l'exemple de la figure 6.5, $\omega = 3$.
- W est le nombre maximal de longueurs d'onde que nous pouvons avoir sur un lien de fibre optique physique. k est un indice qui indique le numéro de la longueur d'onde utilisée et varie entre 1 et W.
- N_l est le nombre de noeuds logiques du réseau.

  - les indices i et j indiquent une paire de noeuds logiques, i et j de 1 à N_l ;
  - les indices o et d indiquent une paire de noeuds origine et destination de flot, o et d de 1 à N_l.
- N_p est le nombre de noeuds physiques du réseau. Les indices l et m indiquent une paire de noeuds physiques, l et m varient de 1 à N_p. Le nombre de noeuds logiques est égal à celui des noeuds physiques, chaque noeud logique i est directement associé à un noeud physique l quand $i = l$.
- Δ est le degré maximal de chaque noeud de la topologie logique. Le degré d'un noeud indique le nombre de liens reliés à ce noeud.
- κ_{max} est la charge de trafic maximale d'un lien logique, c'est la somme des capacités des ω chemins optiques assignés à un lien logique.
- $\lambda^{(od)}$ est un élément de la matrice $N_l \times N_l$ de trafic : $\Lambda = [\lambda^{(od)}]$ où $\lambda^{(od)}$ exprime en unités de trafic la demande entre le noeud logique o au noeud logique d.
- p_{lm} est un indicateur de lien physique. Si $p_{lm} = 1$ un lien physique existe entre les noeuds physiques l et m, 0 sinon.
- h_{ij} : Soit $H = [h_{ij}]$ la matrice des nombres de liens maximal où h_{ij} indique le nombre maximal de liens physiques dans un chemin optique reliant le noeud physique $l = i$ au noeud physique $m = j$.
- P_{ij} est le nombre maximal de chemins physiques disjoints disponibles entre les noeuds logiques i et j.

Les variables du décision

- b_{ij} est un indicateur de canal optique, $b_{ij} = 1$ si la solution met en place au moins un canal optique entre les noeuds logiques i et j, 0 sinon.
- λ_{ij} est la charge de trafic écoulée par le lien logique (i, j). Si $b_{ij} = 0$, le lien (i, j) n'existe pas et $\lambda_{ij} = 0$.
- $\lambda_{ij}^{(od)}$ est la quantité de flot (od) écoulée sur l'arc (i, j).
- c_{ij}^{k} indique le nombre de longueurs d'onde de numéro k utilisées par les chemins optiques mis en place pour créer le lien logique (i, j). $b_{ij} = 0$, le lien (i, j) n'existe pas et

$c_{ij}^{k} = 0$.

- $c_{ij}^{k}[l,m]$ est le routage d'un lien logique (i,j) sur la longueur d'onde k du lien physique $[l,m]$ utilisée. Il indique qu'un des canaux optiques associés au lien logique (i,j) utilise la longueur d'onde k du lien physique entre les noeuds l et m. Cette variable permet le couplage entre les deux couches du réseau.

Reprenons l'exemple du lien logique $(1,5)$ de la figure 6.2 mis en place à l'aide de trois canaux optiques routés sur les chemins physiques $[1,2,5]$, $[1,3,5]$ et $[1,4,5]$. Les variables de décisions associées à cet exemple prendront les valeurs :

- $b_{15} = 1$ parce que le lien logique $(1,5)$ existe ;
- étant donné que la totalité de la demande $\lambda^{(15)}$ est routée sur $(1,5)$ alors $\lambda_{15}^{(15)} = \lambda^{(15)}$;
- étant donné que la totalité de la demande $\lambda^{(26)}$ est routée sur $(2,1,5,6)$ alors $\lambda_{15}^{(26)} = \lambda^{(26)}$;
- la quantité totale de trafic sur $(1,5)$ est $\lambda_{15} = \lambda_{15}^{(15)} + \lambda_{15}^{(26)}$;
- les canaux optiques de $(1,5)$ sont mis en place sur des chemins disjoints. Ils peuvent tous avoir le même numéro de longueur d'onde k ou des valeurs différentes. En supposant $k_{[1,2,5]} = 22$, $k_{[1,3,5]} = 22$ et $k_{[1,2,5]} = 13$ on aura :
  - $c_{15}^{22} = 2$, $c_{15}^{13} = 1$ et $c_{15}^{k \neq 13,22} = 0$
  - $c_{15}^{k}[1,2] = c_{15}^{k}[2,5] = \begin{cases} 1, & si\ k = 22 \\ 0, & sinon \end{cases}$
  - $c_{15}^{k}[1,3] = c_{15}^{k}[3,5] = \begin{cases} 1, & si\ k = 22 \\ 0, & sinon \end{cases}$
  - $c_{15}^{k}[1,4] = c_{15}^{k}[4,5] = \begin{cases} 1, & si\ k = 13 \\ 0, & sinon \end{cases}$

6.2.1.2 Le modèle DiffServ* de routage et d'assignation de longueurs d'onde

Le programme a pour fonction de dimensionner la topologie logique, router la demande de trafic sur cette topologie, déployer DiffServ* sur chacun de ses liens logiques et accomplir l'assignation correspondante des canaux optiques . L'objectif du modèle est de minimiser *le nombre total de longueurs d'onde utilisées dans le réseau.* En minimisant cette valeur, nous réduisons le nombre d'interfaces optiques dans chaque noeud physique du réseau et de ce fait le coût total du réseau.

$$\min_{b,\lambda,c} \sum_{i,j,l,m,k} c_{ij}^{k}[l,m] \tag{6.8}$$

Le *design du réseau logique* constitue un problème de routage de flot avec des contraintes topologiques de capacité et de degré.

Il est possible de limiter le degré de chaque noeud logique et les contraintes suivantes garantissent que le nombre le liens logiques *bidirectionnels* attachés à chaque noeud logique ne dépasse pas une valeur Δ, ainsi :

– le nombre d'arcs sortants du noeud i :

$$\sum_{j} b_{ij} \leq \Delta, \ \forall i \tag{6.9}$$

– le nombre d'arcs entrants au noeud i :

$$\sum_{j} b_{ji} \leq \Delta, \ \forall i \tag{6.10}$$

Des contraintes sur le trafic sont nécessaires. La capacité de chaque lien logique (i,j) est égale à la somme des capacités des ω chemins optiques mis en place entre i et j. La

demande totale trafic sur chaque lien (i, j) (s'il existe) ne doit pas dépasser κ_{max} qui est la capacité maximale d'un lien logique ou bien de ω chemins optiques.

$$\lambda_{ij} \leq \kappa_{max}, \ \forall (i,j) \tag{6.11}$$

Le trafic sur le lien logique (i, j) est égal à la somme de toutes les demandes de trafic entre les noeuds o et d qui utilisent le lien (i, j).

$$\lambda_{ij} = \sum_{od} \lambda_{ij}^{(od)}, \ \forall (i,j) \tag{6.12}$$

Un lien logique (i, j) qui n'existe pas ne peut transporter de trafic.

$$\lambda_{ij}^{(od)} \leq b_{ij} \lambda^{(od)}, \ \forall (i,j),(o,d) \tag{6.13}$$

Nous devons aussi imposer une contrainte de conservation de flot de trafic entre chaque paire de noeud o et d. Le programme permet la division d'un flot et l'envoi de chaque partie sur un chemin logique différent.

$$\sum_j \lambda_{ij}^{od} - \sum_j \lambda_{ji}^{od} = \begin{cases} \lambda^{(od)}, & o = i \\ -\lambda^{(od)}, & d = i \\ 0, & o \neq i, d \neq i \end{cases} \qquad \forall (o,d), i \tag{6.14}$$

Le *design du réseau optique* retrouve pour chacun des canaux optiques des liens logiques un chemin et une longueur d'onde.

Nous voulons mettre en place ω chemins optiques entre les noeuds i and j, chaque canal optique utilise une longueur d'onde spécifique. Cette contrainte réserve ω longueurs d'onde entre les noeuds logiques i et j et permet le couplage entre les deux couches logique et optique du réseau. La mise en place d'un lien logique (i, j) constitue une demande d'établissement de ω canaux optiques au niveau physique et c_{ij}^k donne le nombre de longueurs d'ondes de numéro k qui sont requis. Cette contrainte assure le couplage entre les deux couches du réseau.

$$\sum_k c_{ij}^k = \omega \times b_{ij},\ \forall(i,j) \tag{6.15}$$

Si le lien logique (i, j) n'utilise pas la longueur d'onde k, alors aucune longueur d'onde ayant ce numéro ne doit être réservée sur aucun lien physique $[l, m]$ pour (i, j). Cette contrainte s'exprime par :

$$c_{ij}^k[l,m] \leq c_{ij}^k,\ \forall(i,j),[l,m],k \tag{6.16}$$

La longueur d'onde k du lien physique $[l, m]$ est uniquement réservée pour un canal optique mis en place entre les noeuds logiques i et j. Si le lien physique $[l, m]$ n'existe pas, aucune longueur d'onde ne peut être réservée sur ce lien.

$$\sum_{ij} c_{ij}^k[l,m] \leq p_{lm},\ \forall[l,m],k \tag{6.17}$$

Il faut assurer la continuité d'une longueur d'onde le long d'un canal optique sur un chemin physique. ω chemins optiques sortent du noeud $m = i$ et ω chemins optiques rentrent dans le noeud $m = j$. Il doit y avoir conservation des numéros de longueurs d'onde utilisées par le canaux optiques sur tout noeud intermédiaire $m \neq i$ et $m \neq j$

$$\sum_l c_{ij}^k[l,m]p_{lm} - \sum_l c_{ij}^k(m,l)p_{ml} = \begin{cases} c_{ij}^k, & m = j \\ -c_{ij}^k, & m = i \\ 0, & m \neq i, m \neq j \end{cases} \quad \forall (i,j), m, k \qquad (6.18)$$

Une contrainte qui limite le nombre de liens traversés par un canal optique est nécessaire. La longueur moyenne en nombre de liens d'un chemin optique ne doit pas dépasser une valeur spécifique.

$$\sum_{lm} c_{ij}^k[l,m] \leq \omega \times h_{ij}, \ \forall (i,j), k \qquad (6.19)$$

Il faut empêcher la formation des boucle dans le routage des canaux optiques et s'assurer que les canaux optiques assignés à des numéros identiques de longueur d'onde soient sur des chemins disjoints.

$$\sum_m c_{ij}^k[l,m] \leq \begin{cases} c_{ij}^k, & l = i \\ 1 & l \neq i \end{cases} \quad \forall (i,j), l, k \qquad (6.20)$$

Le déploiement de DiffServ* sur le lien logique (i,j) est assuré par répartition de ses canaux optiques sur le plus grand nombre possible de chemins physiquement disjoints. Si P_{ij} chemins physiques disjoints existent entre les noeuds logiques i et j alors aucun lien du réseau physique ne doit être utilisé plus de $\omega - P_{ij} + 1$ fois pour le lien logique (i,j).

$$\sum_k c_{ij}^k[l,m] \leq (\omega - P_{ij} + 1)b_{ij} \qquad (6.21)$$

6.2.2 Modèle 2 : Déploiement de DiffProtect

Avec une certaine topologie physique et une matrice de trafic, le modèle de la section 6.2.1 est utilisé pour compléter l'architecture du réseau en définissant une topologie logique adéquate, un routage du trafic sur cette topologie logique ainsi qu'une assignation de longueur d'onde qui respecte les conditions de déploiement du modèle de protection DiffServ* sur tout les liens de la topologie logique. En utilisant la probabilité de pannes des liens physiques, nous pouvons calculer la probabilité de pannes simples et multiples qui peuvent avoir lieu sur les canaux optiques des différents liens logiques et protégés par DiffServ*. Pour tous les liens logiques où la probabilité de pannes est inacceptable, la protection DiffServ* peut être remplacée par DiffProtect. L'objectif de ce modèle est alors de déployer DiffProtect sur tous les liens où la situation requiert spécifiquement les garanties de fiabilité plus élevés de DiffProtect.

Le modèle doit conserver les canaux optiques obtenus par le déploiement de DiffServ* sur ces liens et y ajouter des canaux de protection additionnels qui sont préférablement complètement disjoints des ω chemins originaux. Nous simplifions ce modèle en considérant que $\omega = 3$. Dans ce cas, deux canaux de protection doivent être ajoutés, un canal optique pour la protection dédiée du trafic EF et un autre canal de protection partagée pour le trafic AF.

6.2.2.1 Les paramètres et variables de décision du modèle

Ce programme utilise la solution du modèle 1, i.e. le modèle de déploiement de DiffServ* et il remplace DiffServ* par DiffProtect là où la situation le requiert. Nous détaillons ci-dessous les paramètres et les variables requis.

Les paramètres du modèle

- $B = [b_{ij}]$ est la matrice indicatrice de liens logiques, si $b_{ij} = 1$ un lien logique existe entre les noeuds logiques i et j, 0 sinon.
- γ_{ij} est un paramètre binaire qui spécifie la protection utilisée sur chaque lien logique, $\gamma_{ij} = 0$ si (i, j) est protégé par DiffServ*, $\gamma_{ij} = 1$ si le lien (i, j) doit être protégé par DiffProtect.
- $c_{ij}^{k,n}[l, m]$ est un paramètre binaire qui indique si la longueur d'onde k du lien physique $[l, m]$ est utilisée pour le n^{ieme} canal optique de (i, j). Les canaux optiques sont triés par ordre de longueur des chemins physiques sur lesquels ils sont placés. Si $\omega = 3$ alors n peut prendre les valeurs 1, 2 ou 3, le canal optique 1 est réservé pour le trafic EF, le deuxième pour AF et le dernier pour BE.

Il faut noter que $c_{ij}^{k,1}[l, m]$, $c_{ij}^{k,2}[l, m]$ et $c_{ij}^{k,3}[l, m]$ représentent la décomposition par canal optique de la variable $c_{ij}^{k}[l, m]$ calculée par la première partie de ce modèle. Cette décomposition sert à identifier les canaux optiques, la classe de trafic transmis sur chacun et le type de protection qu'ils exigent.

Les variables de décision

- $r_{ij}^{k}[l, m]$ indique si la longueur d'onde k du lien physique $[l, m]$ est utilisée pour un chemin de protection dédiée pour le trafic EF du lien logique (i, j)
- $t_{ij}^{k}[l, m]$ indique si la longueur d'onde k du lien physique $[l, m]$ est utilisée pour un chemin de protection partagée pour le trafic AF du lien logique (i, j)
- r_{ij}^{k} indique si le lien logique (i, j) utilise k comme une longueur d'onde de protection dédiée
- t_{ij}^{k} indique si le lien logique (i, j) utilise k comme une longueur d'onde de protection partagée
- s_{lm}^{k} indique si la longueur d'onde k du lien physique $[l, m]$ est utilisée comme une longueur d'onde de protection partagée

Les variables r_{ij}^{k} et t_{ij}^{k} jouent le rôle de demande de connexion optique. Si (i, j) est protégé

par DiffServ*, $r_{ij}^k = t_{ij}^k = 0$ et aucun canal de protection n'est requis. Si DiffProtect est utilisé sur (i, j), deux canaux de protection sont requis, dédié avec $r_{ij}^k = 1$ pour une seule valeur de k, il en est de même pour $t_{ij}^k = 1$ pour la protection partagée. Les variables $r_{ij}^k[l, m]$ et $t_{ij}^k[l, m]$ assurent la mise en place concrète des canaux de protection.

6.2.2.2 Le modèle de déploiement de DiffProtect

L'objectif du modèle est de minimiser le nombre total de longueurs d'onde de protection utilisées dans le réseau.

$$\min \sum_{i,j,l,m,j} t_{ij}^k[l, m] + \sum_{l,m,k} s_{lm}^k \tag{6.22}$$

Il faut noter que l'objectif tient compte des variables $r_{ij}^k[l, m]$, s_{lm}^k et non de $t_{ij}^k[l, m]$. Pour expliquer ceci, nous considérons l'exemple de deux liens logiques (i, j) et (i', j') protégés par DiffProtect et qui requièrent la mis en place de deux canaux de protection partagée. Supposons que ces canaux traversent le lien (l, m), il doivent alors partager l'utilisation d'une même longueur d'onde k. Nous aurons d'un côté $t_{ij}^k[l, m] = t_{i'j'}^k[l, m] = 1$ et d'un autre $s_{lm}^k = 1$. Si le décompte de longueurs d'onde de la fonction objectif se faisait avec $t_{ij}^k[l, m]$ au lieu de s_{lm}^k, nous compterions alors la même longueur d'onde k du même lien physique $[l, m]$ deux fois, ce qui fausserait les résultats.

Dans tout ce qui suit, nous considérons l'hypothèse qu'il existe au minimum deux chemins physiques disjoints entre toute paire de noeuds. Cette hypothèse est nécessaire pour la mise en place des canaux de protection sur des chemins optiques disjoints de ceux utilisés pour la transmission du trafic en temps normal.

6.2.2.2.1 Les contraintes de la protection dédiée Cette contrainte assure la continuité d'une longueur d'onde le long d'un canal optique de protection sur un chemin physique. Si la protection du lien logique (i, j) est DiffProtect, alors un chemin de protection dédiée sur une longueur d'onde doit être mis en place entre i et j.

$$\sum_l r_{ij}^k[l,m]p_{lm} - \sum_l r_{ij}^k(m,l)p_{ml} = \begin{cases} \gamma_{ij}r_{ij}^k, & m = j \\ -\gamma_{ij}r_{ij}^k, & m = i \\ 0, & m \neq i, m \neq j \end{cases} \quad \forall (i,j), m, k \qquad (6.23)$$

La contrainte définit le nombre de longueurs d'onde réservées pour la protection dédiée. Si le lien (i, j) existe ($b_{ij} = 1$) *et* sa protection est DiffProtect, ce nombre est égal à 1, sa valeur est 0 sinon.

$$\sum_k r_{ij}^k = \gamma_{ij}b_{ij} \; \forall (i,j), [l,m] \qquad (6.24)$$

Nous pouvons avoir au maximum une longueur d'onde de valeur k du lien physique $[l, m]$ qui peut être réservée pour un chemin de protection dédiée pour le lien logique (i, j).

$$r_{ij}^k[l,m] \leq r_{ij}^k, \; \forall (i,j), [l,m], k \qquad (6.25)$$

Puisque le chemin optique le plus court est utilisé pour le trafic EF, le chemin de protection dédiée doit être disjoint de ce dernier. Nous exprimons cette contrainte par :

$$\sum_k r_{ij}^k[l,m] + c_{ij}^{k,1}[l,m] \leq 1 \; \forall (i,j), [l,m] \qquad (6.26)$$

Si nous avons plus que ω chemins physiques disjoints entre les noeuds i et j alors le canal

de protection dédiée doit être mis en place sur le $(\omega+1)^{ieme}$ plus court chemin entre i and j et disjoint des ω canaux optiques de trafic originaux. Cette contraint s'exprime par :

$$Si\ P_{ij} > \omega\ alors \begin{cases} \sum_k r_{ij}^k[l,m] + c_{ij}^{k,2}[l,m] \leq 1 \\ \sum_k r_{ij}^k[l,m] + c_{ij}^{k,3}[l,m] \leq 1 \end{cases} \quad \forall (i,j),[l,m] \qquad (6.27)$$

Si nous avons exactement ω chemins physiques entre les liens logiques i et j, le chemin de protection dédiée doit être mis en place sur le deuxième plus court chemin entre i et j, le même chemin utilisé pour le trafic AF. Aucune contrainte additionnelle n'est requise dans ce cas. Le canal optique de protection dédiée est déjà disjoint de celui du trafic EF et il sera mis en place sur le deuxième plus court chemin, celui de AF.

Il faut aussi prévenir l'usage de la même longueur d'onde d'un lien physique $[l,m]$ comme une longueur d'onde primaire et de protection.

$$\sum_{ij} \left\{ c_{ij}^{k,1}[l,m] + c_{ij}^{k,2}[l,m] + c_{ij}^{k,3}[l,m] + r_{ij}^k[l,m] \right\} + s_{lm}^k \leq p_{lm}\ \forall [l,m],k \qquad (6.28)$$

6.2.2.2.2 Contraintes de la protection partagée Il faut assurer la continuité d'une longueur d'onde le long d'un canal optique de protection sur un chemin physique. Si la protection du lien logique (i,j) est DiffProtect donc un canal de protection partagée sur une longueur d'onde doit être mis en place entre i et j.

$$\sum_l t_{ij}^k[l,m]p_{lm} - \sum_l t_{ij}^k(m,l)p_{ml} = \begin{cases} \gamma_{ij}t_{ij}^k, & m = j \\ -\gamma_{ij}t_{ij}^k, & m = i \\ 0, & m \neq i, m \neq j \end{cases} \quad \forall(i,j), m, k \qquad (6.29)$$

Il faut définir le nombre de longueurs d'onde réservées pour la protection partagée. Si le lien (i,j) existe ($b_{ij} = 1$) *et* sa protection est DiffProtect, ce nombre est égal à 1, sa valeur est 0 sinon.

$$\sum_k t_{ij}^k = \gamma_{ij}b_{ij} \; \forall(i,j),[l,m] \qquad (6.30)$$

Nous pouvons avoir au maximum une longueur d'onde de valeur k du lien physique $[l,m]$ qui peut être réservée pour un chemin de protection partagée pour le lien (i,j). Cette contrainte s'exprime par :

$$t_{ij}^k[l,m] \leq t_{ij}^k, \; \forall(i,j),[l,m],k \qquad (6.31)$$

Puisque le deuxième plus court chemin optique est utilisé pour le trafic AF, le canal de protection partagée doit être disjoint de ce dernier.

$$\sum_k t_{ij}^k[l,m] + c_{ij}^{k,2}[l,m] \leq 1 \; \forall(i,j),[l,m] \qquad (6.32)$$

Si nous avons plus que deux chemins physiques disjoints entre i et j, le chemin de protection partagée doit aussi être disjoint du chemin utilisé pour EF :

$$Si\ P_{ij} \geq \omega\ alors \sum_k t_{ij}^k[l,m] + c_{ij}^{k,1}[l,m] \leq 1\ \forall(i,j),[l,m] \tag{6.33}$$

Si nous avons plus que ω chemins physiques disjoints entre les noeuds i et j, le chemin de protection partagée doit être mis en place sur le $\omega + 1^{ieme}$ plus court chemin entre i and j. Dans ce cas, le chemin de protection partagée est disjoint des ω chemins optiques de trafic originaux.

$$Si\ P_{ij} > \omega\ alors \sum_k t_{ij}^k[l,m] + c_{ij}^{k,3}[l,m] \leq 1\ \forall(i,j),[l,m] \tag{6.34}$$

Plusieurs canaux optiques de protection partagée doivent utiliser la même longueur d'onde s'ils traversent le même lien physique. Puisque nous minimisons le nombre de longueurs d'onde total du réseau, le modèle choisira d'utiliser la même longueur d'un lien physique pour une protection partagée quand c'est possible. Cette contrainte spécifie qu'il est possible d'avoir au maximum une longueur d'onde de protection partagée par lien physique $[l,m]$.

$$\sum_k s_{lm}^k \leq p_{lm}\ \forall l,m \tag{6.35}$$

Si la longueur d'onde de protection partagée du lien logique (i,j) utilise le lien physique $[l,m]$, elle doit donc utiliser la valeur de la longueur d'onde déjà réservée à cet effet. Nous exprimons ceci par la contrainte :

$$t_{ij}^k[l,m] \leq s_{lm}^k\ \forall(i,j),[l,m],k \tag{6.36}$$

Il faut empêcher la formation des boucles dans le routage des canaux optiques de protec-

tion partagée :

$$\sum_{m} t_{ij}^{k}[l,m] \leq 1 \forall (i,j), l, k \tag{6.37}$$

6.2.3 Modèle 3 : Routage de flot avec MixProtect

Une fois la deuxième partie du modèle complétée, il faut minimiser la quantité de trafic EF, AF et BE sur tous les chemins logiques qui ne respectent pas les contraintes de protection de chemin combinée (MixProtect). Nous avons utilisé une approche par pénalité qui est conforme aux observations que nous avons recueillies par simulation. Ces règles d'ingénierie sont les suivantes :

- la variation de la protection du chemin influence très légèrement la performance de la classe EF. En effet, nous observons une augmentation relativement négligeable du taux de perte EF quand le nombre de liens protégés par DiffServ* augmente. Si ces taux de pertes sont inacceptables, il est préférable d'avoir une dominance de DiffProtect sur les chemins utilisés par les flots EF ;
- pour la classe AF, ces contraintes sont :
  - Le dernier lien d'un chemin utilisé par un flot AF doit être protégé par DiffProtect ;
  - Le nombre de liens protégés par DiffServ* sur un chemin particulier ne doit pas dépasser de beaucoup le nombre de ceux protégés par DiffProtect ;
- seul le nombre de liens protégés par DiffProtect influence la performance perçue par les flots BE. Pour diminuer le taux de perte BE, il faut donc avoir un plus grand nombre de liens protégés par DiffServ*. Si le délai et la gigue sont plus importants, DiffProtect est le mécanisme de choix.

6.2.3.1 Notion de pénalité de protection

Il existe pour chaque paire de noeuds origine/destination (o/d) un ensembles de chemins P_{od} qui peuvent être utilisés pour le transport du trafic. Chaque chemin est protégé par une combinaison DiffServ*/DiffProtect connue. Nous utilisons une approche par pénalité pour suivre les règles d'ingénierie qui influencent le déploiement de MixProtect dans un réseau donné. La pénalité est calculée en utilisant la quantité et la classe de trafic routé sur un chemin. La qualité d'un chemin est évalué en utilisant deux critères, l'un, α_p^{od}, qui dépend de la *position* des liens protégés par DiffProtect dans un chemin en particulier, l'autre, β_p^{od}, qui est le nombre moyen de liens protégés par DiffProtect et par DiffServ*.

Nous calculons α_p^{od} comme étant une valeur de pénalité normalisée sur la longueur du chemin et associée à la position des liens protégés par DiffProtect sur un chemin $p \in P_{od}$ entre o et d à partir de l'équation :

$$\alpha_p^{od} = \frac{\sum_{(i,j)\in p,\, \gamma_{ij} n_{ij}^p}}{\sum_{(i,j)\in p} n_{ij}^p} \; p \in P_{od} \tag{6.38}$$

Où n_p, n_{ij}^p et γ_{ij} sont définis comme étant :

- n_p est le nombre de liens, du chemin $p \in P_{od}$
- n_{ij}^p indique la position du lien (i,j) dans le chemin $p \in P_{od}$, $n_{ij}^p = 0$ si le lien $(i,j) \notin p$, $n_{ij}^p = 1$ si (i,j) est le premier lien du chemin p, $n_{ij}^p = 2$ s'il est le deuxième, etc.
- γ_{ij} est un paramètre binaire qui spécifie la protection utilisée sur chaque lien logique, $\gamma_{ij} = 0$ si (i,j) est protégé par DiffServ*, $\gamma_{ij} = 1$ si le lien (i,j) doit être protégé par DiffProtect.

Une valeur élevée de α_p^{od} indique que DiffProtect protège les liens qui se trouvent à la fin du chemin alors qu'une valeur faible indique que les liens protégés par DiffProtect sont

au début. $\alpha_p^{od} = 0$ quand tous les liens du chemin p sont protégés par DiffServ*.

Le coût β_p^{od} est le nombre moyen de liens protégés par DiffProtect et est donné par :

$$\beta_p^{od} = \frac{\sum_{(i,j)\in p} \gamma_{ij}}{n_p} \; p \in P_{od} \tag{6.39}$$

Ainsi, plus la valeur de β_p^{od} est élevée plus le nombre de liens protégés par DiffProtect est élevé. $\beta_p^{od} = 0$ quand tous les liens sont protégés par DiffServ*

La pénalité d'un flot sur un chemin $p \in P_{od}$ donné dépend non seulement des valeurs de α_p^{od} et β_p^{od} mais aussi de la quantité et la classe de trafic X_p^k sur ce chemin où $k \in [EF, AF, BE]$.

6.2.3.2 Les paramètres et variables du modèle

Les paramètres du modèle

- P_{od} est l'ensemble des chemins logiques qui relient tout noeud origine o à tout noeud destination d.
- $p \in P_{od}$ est un des chemins logiques entre o et d.
- x_p^k est la portion originale de trafic de classe $k \in [EF, AF, BE]$ entre la source o et la destination d routée sur le chemin $p \in P_{od}$.
- $\lambda^{(od),k}$ est la demande de trafic de classe $k \in [EF, AF, BE]$ entre le noeud logique o et le noeud logique d. Nous avons :

$$\sum_{k\in[EF,AF,BE]} \lambda^{(od),k} = \lambda^{(od)} \tag{6.40}$$

- α_p^{od} est une valeur de coût normalisée sur la longueur du chemin et associée à la position

des liens protégés par DiffProtect sur un chemin $p \in P_{od}$ entre o et d.

- β_p^{od} est une valeur de coût associée au nombre de liens protégés par DiffProtect versus ceux protégés par DiffServ* sur un chemin $p \in P_{od}$ entre o et d.

Les variables du modèle

- x_p^k est la quantité de trafic $k \in [EF, AF, BE]$ routée sur le chemin $p \in P_{od}$

6.2.4 Le modèle d'optimisation

Il est nécessaire de mentionner que nous choisissons une approche *par chemin* pour ce modèle de routage multiflot avec contraintes de capacité plutôt qu'une méthode *par lien* comme celle utilisée précédemment dans le modèle des sections 6.2.1 et 6.2.2. Nous justifions ceci par le fait que nous avons besoin de l'information sur tout le chemin utilisé par un flot particulier et non seulement de celle de chacun des liens individuels du réseau pour pouvoir évaluer adéquatement la pénalité due au routage et donc la fonction objectif du modèle. La modélisation par lien serait simplement inadéquate puisque la pénalité de protection par chemin est inaccessible dans ce cas.

D'après les résultats de simulation, nous savons que la performance d'un flot EF n'est pas affectée par la position des liens protégés par DiffProtect mais seulement et très faiblement par leur nombre. En effet, le taux de pertes de paquets EF augmente très légèrement avec le nombre de chemins protégés par DiffServ*. Un flot AF est affecté autant par le nombre et la position des liens protégés par DiffProtect. Le nombre de chemins qui utilisent DiffServ* doit être proche du nombre de chemins qui utilisent DiffProtect et c'est ce dernier qui doit couvrir la dernière portion du chemin parcouru par un flot AF. Un flot BE est surtout affecté par le nombre de liens protégés par DiffProtect et non leur position. Si nous voulons minimiser le taux de pertes de ce flot, tous les liens doivent être protégés par DiffServ*. Si c'est le délai de bout-en-bout et la gigue qui sont visés, DiffProtect doit

être le mécanisme de choix.

En utilisant ces règles de déploiement il faut :

- minimiser la quantité de trafic EF sur les chemins où $1-\beta$ est élevé ;
- minimiser la quantité de trafic AF sur les chemins où $1-\alpha$ et $1-\beta$ sont élevés ;
- minimiser la quantité de trafic BE sur les chemins où β est élevé.

Nous pouvons ainsi déduire la pénalité par chemin de chaque flot :

$$X_p = (1-\beta_p^{od})x_p^{k=EF} + ((1-\alpha_p^{od}) + (1-\beta_p^{od}))x_p^{k=AF} + \beta_p^{od}x_p^{k=BE} \tag{6.41}$$

Étant donné que la coût de chaque chemin n'est pas calculée en additionnant les coûts individuels de tous ses liens, nous ne pouvons utiliser un simple algorithme de plus court chemin, Dijkstra par exemple, pour router les flots dans le réseau. Pour réaliser le routage, nous utilisons le modèle d'optimisation suivant dont la fonction objectif est définit par :

$$\min \sum_{(o,d)} \sum_{p \in P_{od}} X_p \tag{6.42}$$

Il faut en premier lieu s'assurer que la totalité de la demande de trafic de classe k entre deux noeuds o et d est acheminée, ainsi :

$$\sum_{p \in P_{od}} x_p^k = \lambda^{(od),k} \; k \in [EF, AF, BE] \tag{6.43}$$

Ensuite, le routage par flot doit être réalisé en respectant la capacité κ_{max} des liens logiques du réseau. La charge de trafic de classe $k \in [EF, AF, BE]$ sur chaque lien se calcule par

$$\lambda_{ij}^{k} = \sum_{p \; qui \; contient \; (i,j)} x_p^k \; \forall (i,j,k) \tag{6.44}$$

Ayant λ_{ij}^{k}, nous pouvons calculer la quantité de trafic totale sur chaque lien (i,j) :

$$\lambda_{ij} = \sum_{k \in [EF,AF,BE]} \lambda_{ij}^{k} \; \forall (i,j) \tag{6.45}$$

La contrainte de capacité pour chaque lien (i,j) devient :

$$\lambda_{ij} \leq \kappa_{max} \; \forall (i,j) \tag{6.46}$$

Pour résoudre ce problème, il faut calculer au préalable un sous-ensemble de chemins candidats P_{od} pour chaque paire de noeuds logiques o et d. Cette tâche peut être irréalisable et inefficace pour des grands réseaux. La résolution par génération de colonne est alors envisageable pour résoudre des problèmes de très grande taille. Dans cette méthode, les différents chemins possibles sont générés au fur et à mesure que le processus d'optimisation le requiert.

6.2.5 Technique de solution par détournement de flot

Au cours de l'étape de déploiement de DiffServ* nous avons procédé au design de la topologie logique et au routage de la demande de trafic sur cette dernière. Ce routage de flot est valide tant et aussi longtemps que la protection DiffServ* est utilisée sur tous les liens logiques du réseau. Après avoir remplacé DiffServ* par DiffProtect dans certains endroits, il est possible d'appliquer une technique de détournement de flot sur le routage calculé préalablement pour minimiser la pénalité du réseau. Cette technique de solution

permet au concepteur du réseau de réévaluer le routage de façon progressive en fonction des changements singuliers ou multiples de la protection sur un ou plusieurs liens du réseau.

Il faut en premier lieu évaluer la solution de routage initiale pour ensuite procéder par le détournement de flot. La solution du modèle de la section 6.2.1 nous donne le routage en termes de quantité de trafic *par lien* logique du réseau. Dans l'exemple de la figure 6.6, les valeurs de routage du flot de 12 unités de trafic de $o = 1$ à $d = 4$ sont suivantes.

- $\lambda_{ij}^{14} = 3$ unités de trafic pour $(i, j) \in [(1, 2), (3, 4)]$;
- $\lambda_{ij}^{14} = 12$ unités de trafic pour $(i, j) = 2, 3)$;
- $\lambda_{ij}^{14} = 9$ unités de trafic pour $(i, j) \in [(1, 5), (5, 2), (3, 6), (6, 4)]$;

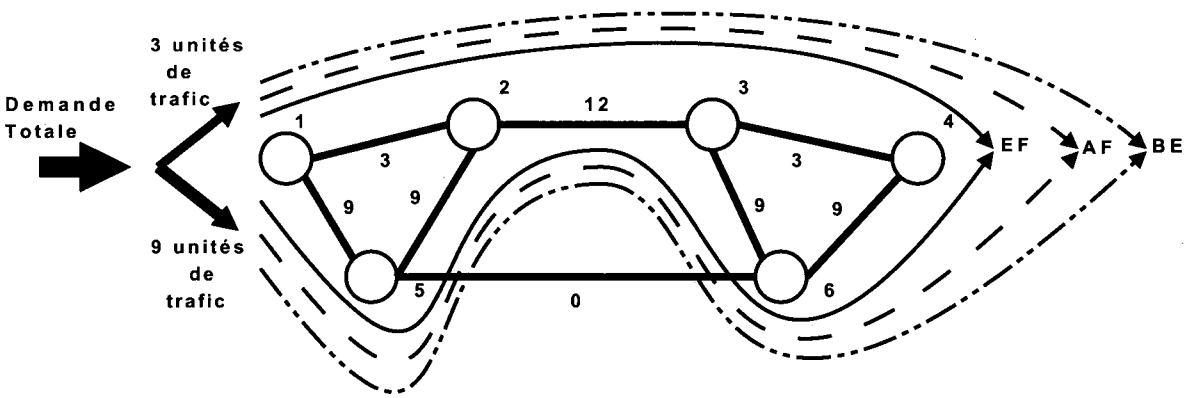


FIG. 6.6 Solution de routage par lien VS. par chemin

Pour traduire cette information de routage en fonction d'une quantité de trafic *par chemin* logique attribuable à une paire (o, d) *spécifique*, il faut :

- considérer un premier chemin $(1, 2, 3, 4)$ entre o et d ;
- retrouver la quantité de trafic sur chacun de ses lien. Dans ce cas, nous avons respectivement les valeurs 3, 12, et 3 ;
- calculer le minimum de ses valeurs et déduire 3 unités de trafic du flot entre 1 et 4 qui sont routés sur ce chemin ;

- réduire de 3 la quantité de trafic sur chacun des liens de $(1, 2, 3, 4)$;
- répéter le même processus jusqu'à ce que la règle de conservation de flot soit satisfaite, c'est à dire que la somme des flots sur tous les chemins trouvés soit égale à la demande (o, d) initiale.

Il est à noter qu'il peut exister plusieurs solutions de routage de flot par chemin qui correspondent à une même solution de routage de flot par lien. Pour l'exemple de la figure 6.6, deux solutions sont possibles. La première est telle qu'illustrée, la demande totale est divisée sur deux chemins : 3 unités de trafic sur $(1, 2, 3, 4)$ et 9 sur $(1, 5, 2, 3, 6, 4)$. La deuxième solution est comme suit : 3 unités sur $(1, 2, 3, 6, 4)$, 3 sur $(1, 5, 2, 3, 4)$ et 6 sur $(1, 5, 2, 3, 6, 4)$. Les deux solutions sont valides et l'utilisation de l'un ou l'autre comme solution initiale n'affectera pas la solution finale parce que nous procédons ici par *détournement de flot*. Quelle que soit la solution initiale, le routage sera réévalué de façon à obtenir une solution finale et optimale.

La composition EF, AF et BE des différents flots en combinaison avec la valeur λ_{ij}^{od} nous permet de déduire $\lambda_{ij}^{od,k}$, $k \in [EF, AF, BE]$ définies comme étant les portions respectives de flot EF, AF et BE de λ_{ij} dues à la demande de trafic entre o et d avec :

$$\lambda_{ij}^{od} = \sum_{k \in [EF,AF,BE]} \lambda_{ij}^{od,k} \tag{6.47}$$

En tenant compte de $\lambda_{ij}^{od,k}$ et de la discussion précédente sur la transition du routage par lien à celui par chemin, nous pouvons déduire la solution initiale de routage y_p^k comme étant la fraction de trafic de classe $k \in [EF, AF, BE]$ entre la source o et la destination d routée sur le chemin $p \in P_{od}$.

Sachant que l'objectif est toujours :

$$\min \sum_{(o,d)} \sum_{p \in P_{od}} X_p \tag{6.48}$$

Avec :

$$X_p = (1 - \beta_p^{od}) x_p^{k=EF} + ((1 - \alpha_p^{od}) + (1 - \beta_p^{od})) x_p^{k=AF} + \beta_p^{od} x_p^{k=BE} \tag{6.49}$$

Il faut maintenant tenir compte des variables de détournement de flot suivantes pour calculer x_p^k :

- Δ_p^{k+} est la quantité de trafic de classe $k \in [EF, AF, BE]$ ajoutée au chemin $p \in P_{od}$.
- ϕ_p^{k+} est une variable binaire de valeur 1 si du trafic de classe k a été ajouté au chemin p, 0 sinon.
- Δ_p^{k-} est la quantité de trafic de classe $k \in [EF, AF, BE]$ ajoutée au chemin $p \in P_{od}$.
- ϕ_p^{k-} est une variable binaire de valeur 1 si du trafic de classe k a été ajouté au chemin p, 0 sinon.

Nous avons :

$$x_p^k = y_p^k + \phi_p^{k+} \Delta_p^{k+} + \phi_p^{k-} \Delta_p^{k-} \tag{6.50}$$

L'évaluation de la fonction objectif est sujette aux contraintes de détournement de flot. Les variables ϕ_p^{k+} et ϕ_p^{k-} doivent être mutuellement exclusives c'est à dire qu'il ne devrait pas être possible d'enlever et d'ajouter du flot de type $k \in [EF, AF, BE]$ à un même chemin en même temps :

$$\phi_p^{k+} + \phi_p^{k-} \leq 1 \; \forall p \in P_{od} \; et \; \forall (o, d, k) \tag{6.51}$$

Étant donné que la quantité de flot de classe $k \in [EF, AF, BE]$ enlevée du chemin $p \in P_{od}$ doit être inférieure à la quantité de flot qui s'y trouve déjà, nous avons la contrainte :

$$\Delta_p^{k-} \leq \phi_p^{k-} x_p^k \; \forall p \in P_{od} \; et \; \forall (o,d,k) \tag{6.52}$$

Nous réutilisons les équations 6.44 et 6.45 pour calculer la charge de trafic λ_{ij} du lien logique (i,j) et la contrainte de capacité s'exprime par :

$$\lambda_{ij} \leq \kappa_{max}, \; \forall (i,j) \tag{6.53}$$

Il est possible de décomposer cette dernière contrainte en fonction de la proportion de trafic acceptable sur chaque lien logique pour chaque classe de trafic. Cette contrainte est beaucoup plus appropriée pour les liens protégés par DiffProtect puisque le trafic d'une classe $k \in [EF, AF, BE]$ de trafic est transmis sur un canal optique dédié, le partage des canaux de transmission entre les classes n'est pas permis. Dans le cas ci-contre nous avons trois classes de trafic sur $\omega = 3$ canaux optiques.

$$\lambda_{ij}^k \leq \frac{\kappa_{max}}{\omega}, \; \forall (i,j,k) \tag{6.54}$$

Nous avons besoin aussi de contraintes qui connectent les variables binaires ϕ_p^{k+} aux variables de détournement de flot Δ_p^{k+}. Seulement dans le cas où ϕ_p^{k+} est égale à 1 qu'il est possible d'ajouter du trafic de cette classe à un lien et quelque soit la situation, la quantité de trafic maximale que nous puissions ajouter est toujours inférieure à la capacité κ_{max} de tout lien du réseau.

$$\Delta_p^{k+} \leq \phi_p^{k+} \kappa_{max} \; \forall p \in P_{od} \; et \; \forall (o,d,k) \tag{6.55}$$

Une contrainte de conservation de flot finale est nécessaire, la quantité de flot de classe

$k \in [EF, AF, BE]$ enlevée de certains chemins doit être compensée par un ajout sur d'autres chemins entre o et d.

$$\sum_{p \in P_{od}} \phi_p^{k+} \Delta_p^{k+} = \sum_{p \in P_{od}} \phi_p^{k-} \Delta_p^{k-}, \ \forall (o, d) \tag{6.56}$$

6.3 Implémentation et résultats

Les trois modèles des sections précédentes ont été implémentés en utilisant le langage AMPL et résolus à l'aide de CPLEX. À l'aide d'une topologie physique fixe et d'une matrice de trafic IP, la première partie du modèle dimensionne la topologie logique, effectue le routage du trafic sur cette dernière et déploie DiffServ* sur chacun de ses liens. Ce déploiement est sujet à la condition que les canaux optiques associés à chaque lien logique protégé par DiffServ* doivent être mis en place sur le plus grand nombre de chemins physiques disjoints disponibles. La solution de cette première partie est fournie comme paramètre au deuxième modèle. En plus de l'assignation et du routage de longueurs d'onde calculé pour la topologie logique entièrement protégée par DiffServ*, il est nécessaire de fournir à ce modèle l'emplacement de DiffProtect dans la topologie logique. Pour chaque lien maintenant protégé par DiffProtect, le modèle déploie deux canaux optiques de protection disjoints l'un pour le trafic EF et l'autre pour AF. Les deux premiers modèles utilisent une approche de déploiement de DiffServ* et DiffProtect et de routage de trafic par lien, leur objectif est de minimiser la quantité de ressources optiques utilisées. Le troisième modèle requiert comme paramètres le routage des flots initial et la protection MixProtect du réseau utilise une approche de routage différenciée par chemin pour optimiser la protection du trafic dans le réseau.

Nous présentons dans cette section un exemple de solution pour un réseau de 10 noeuds pour lequel la topologie physique et la matrice de trafic IP ont été générées aléatoirement.

L'objectif étant de démontrer que le modèle mathématique en trois étapes est fonctionnel et permet effectivement d'optimiser le déploiement de la solution multi-niveau DiffServ*/DiffProtect à la fois en terme de coût et en qualité de protection

6.3.1 Réseau et données initiaux du modèle

Le réseau physique généré aléatoirement pour cette étude est illustré à la figure 6.7. Chaque noeud de cette topologie est à la fois un commutateur optique et un routeur IP. Le tableau 6.1 montre la matrice des demandes de trafic entre les différentes paires de routeurs.

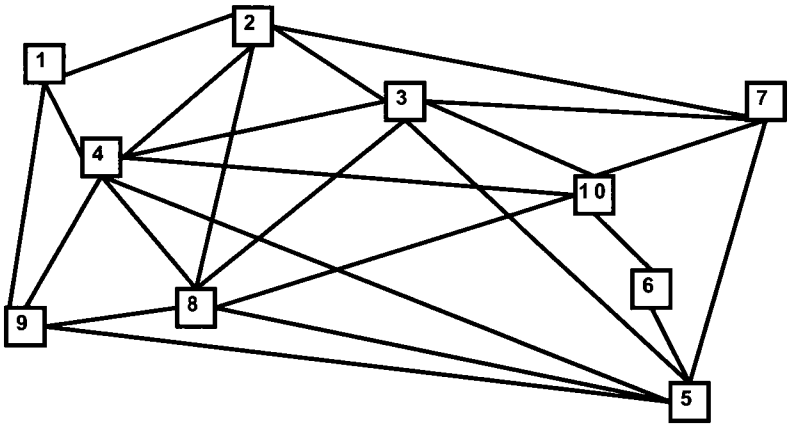


FIG. 6.7 Topologie physique

6.3.2 Routage de flot, topologie logique et déploiement de DiffServ*

La résolution de cette partie du modèle a nécessité près de 62 heures de calcul et la solution obtenue est à 4.55% de la solution de relaxation. La topologie logique calculée par le modèle est illustrée à la figure 6.8. La majorité des routeurs sont reliés par des liens logique unidirectionnels de capacité 30 Gbps. Seuls les liens $(5, 6)$ et $(8, 10)$ sont bidirectionnels, leur capacité est de 30 Gbps dans chaque direction.

Src \ Dest	1	2	3	4	5	6	7	8	9	10
1	0	0	0	**10**	**6**	**4**	0	0	**14**	**3**
2	**9**	0	0	**6**	**11**	**9**	**7**	**6**	**8**	0
3	**1**	0	0	0	0	0	0	0	**14**	**10**
4	0	0	0	0	**5**	0	**4**	**10**	0	**9**
5	**11**	0	**5**	0	0	**10**	**2**	**12**	**14**	**11**
6	**8**	**14**	**11**	**13**	**14**	0	**2**	0	0	**6**
7	**13**	0	0	0	**7**	**9**	0	0	0	0
8	**1**	**14**	**7**	**10**	**9**	0	**3**	0	**7**	**13**
9	**5**	**2**	**8**	**11**	**6**	0	0	0	0	0
10	0	0	0	0	0	**10**	**6**	0	**9**	0

TAB. 6.1 Matrice de trafic (Gbps)

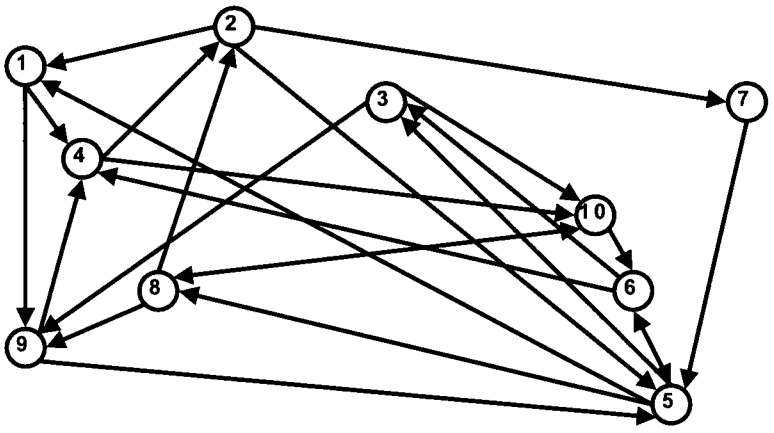


FIG. 6.8 Topologie logique

Source	Destination	Débit(Gbps)	Chemin logique
1	5	6	$1 \rightarrow 9 \rightarrow 5$
4	8	10	$4 \rightarrow 10 \rightarrow 8$
6	2	14	$6 \rightarrow 4 \rightarrow 2$ (12.75 Gbps) $6 \rightarrow 5 \rightarrow 8 \rightarrow 2$ (1.25 Gbps)

TAB. 6.2 Routage des flot

Lien	1	2	3	4	5	6	7	8	9	10
1	0	0	0	**0.73**	0	0	0	0	**0.89**	0
2	1	0	0	0	**1**	0	**0.83**	0	0	0
3	0	0	0	0	0	0	0	0	**1**	**0.72**
4	0	**0.97**	0	0	0	0	0	0	0	**1**
5	**0.99**	0	**1**	0	0	**1**	0	**0.98**	0	0
6	0	0	**0.92**	**1**	**0.95**	0	0	0	0	0
7	0	0	0	0	**1**	0	0	0	0	0
8	0	**1**	0	0	0	0	0	0	**1**	**1**
9	0	0	0	**0.97**	**0.79**	0	0	0	0	0
10	0	0	0	0	0	**1**	0	**0.82**	0	0

TAB. 6.3 Matrice des taux d'utilisation des liens

Un exemple du routage de la demande de trafic dans la couche logique est montré au tableau 6.2.

Le tableau 6.3 montre le taux d'utilisation des différents liens logique du réseau. Ce taux est calculé en divisant la charge de trafic sur chaque lien par sa capacité. Un taux d'utilisation moyen de 0.94 montre que le routage a été accompli de façon optimale en minimisant tout gaspillage de ressources de transmission.

La figure 6.9 montre une partie de la solution du routage des canaux optiques sur le plus grand nombre de chemins physiques disjoints. Nous pouvons voir que les canaux optiques du lien logique $(1, 4)$ sont routés sur les chemins physiques $[1, 4]$, $[1, 2, 4]$ et $[1, 9, 4]$ et sont assignés aux numéros de longueur d'onde 26, 21 et 2. Les canaux du lien $(3, 9)$ sont routés sur trois chemins disjoints ; deux sont assignés à la longueur d'onde 27 et le troisième au numéro 8. Ceci montre que le programme permet à deux canaux optiques disjoints d'un

même lien logique d'utiliser le même numéro de longueur d'onde. Il n'est cependant pas le cas des deux canaux optiques non disjoints du lien logique $(10, 6)$. Les deux sont mis en place sur le chemin physique $[10, 6]$ et sont assignés à des longueurs d'ondes différentes : 2 et 8.

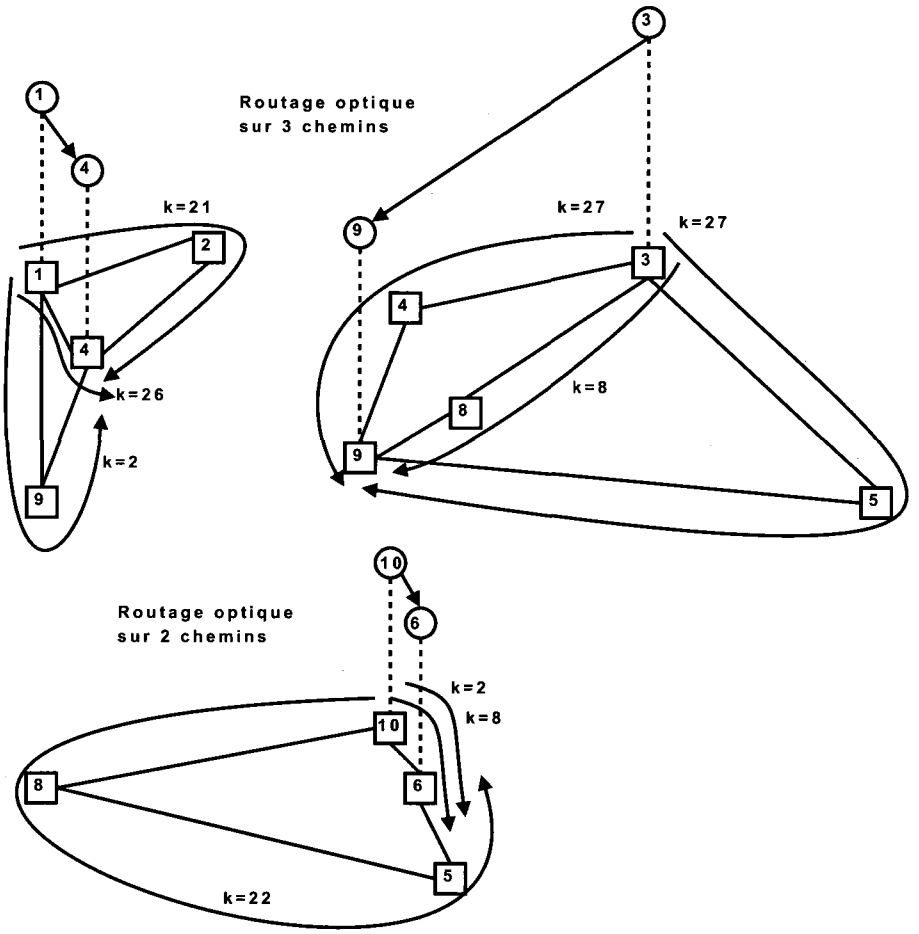


FIG. 6.9 Routage DiffServ* des canaux optiques

6.3.3 Déploiement de DiffProtect

La topologie logique, le routage et l'assignation des longueurs des canaux optiques de tous les liens DiffServ* ainsi que la position des liens qui doivent être protégés par DiffProtect sont fournis au modèle 2. Dans le tableau 6.4, une valeur égale à 1 indique que le lien est

Lien	1	2	3	4	5	6	7	8	9	10
1	0	0	0	1	0	0	0	0	0	0
2	1	0	0	0	1	0	1	0	0	0
3	0	0	0	0	0	0	0	0	0	0
4	0	1	0	0	0	0	0	0	0	0
5	1	0	0	0	0	1	0	0	0	0
6	0	0	1	1	1	0	0	0	0	0
7	0	0	0	0	1	0	0	0	0	0
8	0	1	0	0	0	0	0	0	0	1
9	0	0	0	0	0	0	0	0	0	0
10	0	0	0	0	0	0	0	1	0	0

TAB. 6.4 Matrice des positions de DiffProtect

protégé par Diffprotect, une valeur 0 est attribuée à un lien qui n'existe pas ou qui existe mais est protégé par DiffServ*.

La figure 6.10 montre un exemple de solution du déploiement de DiffProtect. La solution est optimale et a été atteinte en approximativement 4 minutes. Pour le lien logique $(1, 4)$, les canaux de protection dédiée et partagée sont mis en place sur le chemin physique $[1, 9, 4]$ qui est disjoint des canaux EF et AF principaux. Étant donné qu'il existe plus que trois chemins disjoints entre les noeuds 2 et 7, les canaux de protection sont disjoints des trois canaux EF, AF et BE principaux. Les canaux de protection partagée des liens logiques $(1, 4)$ et $(2, 7)$ traversent tous deux les chemins physiques $[1, 9, 4]$ et sont assignés à la même longueur d'onde.

6.3.4 Reroutage des flots pour minimiser la pénalité

Nous avons utilisé la technique de reroutage par détournement de flot pour tenter de minimiser la pénalité du réseau et de maximiser la protection de chacun des flots du réseau. La pénalité du routage des flots initial qui a été évalué lors du déploiement de DiffServ*, était de 264111. Après avoir modifié la protection du réseau à l'étape 2 et après avoir appliqué

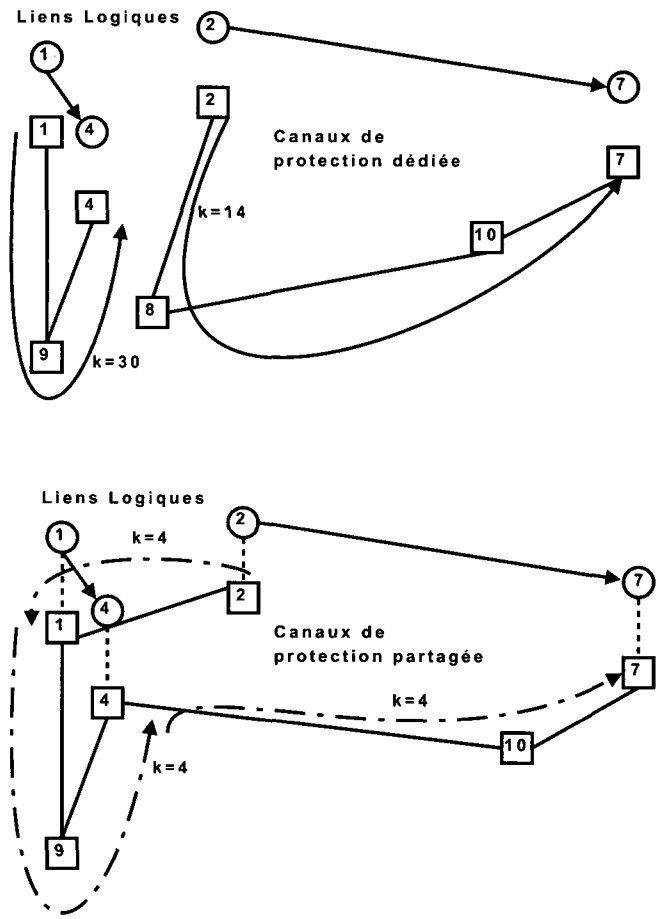


FIG. 6.10 Routage DiffProtect des canaux optiques de protection

			Routage initial			Après détournement		
Classe	Src	Dst	Débit	Chemin	Pénalité	Débit	Chemin	Pénalité
EF	2	4	1667	$(2,1,4)$	0	2000	$(2,1,4)$	0
			333	$(2,7,5,8,9,4)$	200			
AF	5	3	1667	$(5,3)$	3333	1000	$(5,3)$	2000
						667	$(5,6,3)$	0
BE	8	5	583	$(8,2,5)$	583	0	$(8,2,5)$	0
			1250	$(8,9,5)$	0	1667	$(8,9,5)$	0
			1167	$(8,10,6,5)$	778	1333	$(8,10,6,5)$	889
Total					4894			2889

TAB. 6.5 Détournement de flot, exemples

la technique de détournement de flot de l'étape, cette pénalité est devenue 260322. Cette solution est optimale et a été obtenue presque instantanément. Seulement certains flots ont été reroutés, le tableau 6.5 montre quelques exemples. Dans le cas du flot EF entre les noeuds 2 et 4, tout le trafic a été détourné vers le chemin $(2,1,4)$ protégé entièrement par DiffProtect. Pour le flot AF, une partie à été détournée vers le chemin $(5,6,3)$ aussi entièrement protégé par DiffProtect. Nous avons observé l'inverse pour BE, les chemin $(8,9,5)$ et $(8,10,6,5)$ qui sont protégés par DiffServ* respectivement de façon totale et partielle sont maintenant privilégiés.

CONCLUSION

Le modèle DiffServ* de protection différenciée se distingue par sa capacité de traduire toute panne physique en une congestion à la couche logique d'un réseau. Cette caractéristique innovatrice permet aux mécanismes naturels de l'architecture des services différenciées, parties intégrantes de DiffServ*, de protéger chaque classe de trafic selon sa priorité et ses exigences en qualité de service. Ainsi, la proposition d'un modèle de protection basée sur l'utilisation conjointe de DiffServ et de la technique d'agrégation de liens est non seulement fonctionnelle, mais potentiellement moins complexe, moins coûteuse et plus fiable que tout autre mécanisme de protection, notamment physique, présentement envisageable. La simulation séparée du modèle DiffServ* et de son homologue physique DiffProtect renforce cette hypothèse et démontre que dans la majorité des cas, la protection DiffServ* est meilleure que celle offerte par les mécanismes de la couche physique. Nous avons généralisé cette étude par la simulation de réseaux plus complexes, de tailles différentes qui sont entièrement protégés par DiffServ*, par DiffProtect ou par une combinaison des deux, MixProtect. Les résultats ont encore une fois démontré que la qualité de protection de DiffServ* est *en moyenne* supérieure à celle de DiffProtect ; il existe cependant certaines situations particulières où la protection DiffProtect peut en partie s'avérer plus désirable.

En complément à l'étude par simulation, nous avons analysé DiffServ* du point de vue de la fiabilité d'un réseau démuni de tout mécanisme de protection optique. Les résultats ont montré que DiffServ* permet d'augmenter considérablement la fiabilité et la robustesse de la couche logique en cas de pannes physiques. Une analyse de coût a par la suite démontré que toute tentative d'augmenter la fiabilité d'un réseau IP/WDM par le biais de mécanismes de protection physiques ou par DiffProtect s'avère économiquement défavorable ; DiffServ* demeure toujours le plus avantageux en consommation de ressources.

Nous poursuivons ce projet de recherche doctoral par une démonstration de la faisabilité de DiffServ* à l'aide de l'équipement réseau en laboratoire. L'inaccessibilité de la technologie optique nous a poussé vers la technologie Ethernet. Malgré toutes les limitations et les divergences techniques de cette dernière et notre modèle théorique, nous avons réussi à coupler la différenciation de service logique à l'agrégation de liens physiques pour obtenir un DiffServ* pratique fonctionnel et capable de protéger le trafic de hautes priorités en cas de pannes dans le réseau. Ceci témoigne autant de la facilité et de la faible complexité du déploiement de DiffServ* que de son adaptabilité à toute technologie de réseau qui réponds à ses exigences de base.

Finalement, les résultats de simulation de la protection multicouche MixProtect nous ont permis d'extraire des directives de déploiement combiné de DiffServ* et DiffProtect dans un même réseau. En lumière des conclusions de ces études, nous avons élaboré une étude théorique de planification complétée par un modèle mathématique qui a pour objectif d'optimiser le déploiement de DiffServ* et DiffProtect dans tout réseau IP/WDM pour assurer la meilleure protection possible. Cette procédure de déploiement solutionne trois problèmes particulièrement nouveaux ; le premier porte sur le déploiement de deux types de protection sur les liens de la couche logique, le deuxième sur le routage de connexions optiques sur des chemins physiques disjoints et le troisième sur le routage différencié des flots dans la couche logique. En partant d'une topologie physique et d'une matrice de demande de trafic, l'étape 1 de la procédure dimensionne la topologie logique, effectue un routage par lien de la demande de trafic et effectue un déploiement généralisé de DiffServ* dans le réseau complet. En tenant compte des contraintes topologiques et de la vulnérabilité face aux pannes physiques de certains liens logiques du réseau, l'étape 2 substitue DiffServ* pour DiffProtect à ces endroits. Bien que l'objectif des deux premières étapes était de minimiser la quantité de ressources optiques nécessaires au déploiement de MixProtect, l'étape 3 utilise une approche par pénalité pour maximiser la protection en cas de pannes de chaque classe de trafic en effectuant un routage différencié par flot.

Un déploiement généralisé de DiffServ* au sein des réseaux multiservice permet à la fois :

- d'offrir à chaque classe de service une protection contre la congestion logique *et* les pannes physiques faite sur mesure ;
- d'augmenter considérable la fiabilité de la topologie logique et sa robustesse face aux pannes multiples sans avoir recours à des mécanismes de protection physiques ;
- d'effectuer des économies importantes en ressources physiques de transmission ;
- de réduire la complexité et la gestion des réseaux puisque :
  - les exigences de DiffServ* sont facilement disponibles dans la plupart des réseaux contemporains,
  - l'occurrence d'une panne est traitée localement, en temps et lieu, par la couche logique et sans besoin de signalisation externe ou d'intervention humaine.

Les résultats de cette recherche sont suffisamment concluants pour suggérer l'usage de DiffServ* comme mécanisme de protection différenciée principal pour le réseau Internet de prochaine génération. Dans les situations particulières où la protection physique est absolument essentielle, nous proposons DiffProtect. Notre procédure de planification suggère une méthodologie qui optimise le déploiement combiné des deux types de protection dans un même réseau. Étant donné que cette dernière est ultimement basée sur des résultats de simulations, il serait alors souhaitable d'élaborer un modèle complet de déploiement de MixProtect qui soit entièrement analytique et qui tienne compte d'une relation mathématique unique entre :

- la probabilité des pannes ;
- les caractéristiques des deux modèles de protection ;
- les exigences en qualité de service et de protection de chaque classe de trafic.

Ce modèle analytique accompagné d'une preuve du déploiement et de la performance de DiffServ* dans un réseau optique réel constituent des axes de recherches futurs et forment les prochaines étapes dans l'évolution de la protection DiffServ* du trafic.

RÉFÉRENCES

(2002). Link aggregation according to IEEE 802.3ad. SysKonnect white paper.

Alshaer, H. and Horlait, E. (2004). Expedited forwarding end to end delay jitter in the differentiated services networks. In *Proc. IEEE International Conference on High Speed Networks and Multimedia Communications*, pages 14–25.

Arakawa, S., Katou, J., and Murata, M. (2003). Design method of logical topologies with quality of reliability in WDM networks. *Photonic Network Communications*, **5**(2), 107–21.

Awad, C., Sansò, B., and Girard, A. (2008). Diffserv for differentiated reliability in meshed IP/WDM networks. *Computer Networks*, **52**(10), 1988–2012.

Banerjee, A., Drake, J., Lang, J., Turner, B., Kompella, K., and Rekhter, Y. (2001). Generalized multiprotocol label switching : an overview of routing and management enhancements. *IEEE Communications Magazine*, **39**(1), 144–50.

Bennett, J., Benson, K., Charny, A., Courtney, W., and LeBoudec, J.-Y. (2001). Delay jitter bounds and packet scale rate guarantee for expedited forwarding. *Proc. IEEE INFOCOM*, **3**, 1502–1509.

Bensaou, B., Shixin, Z., and Xiren, C. (2004). Statistical bounds on the drop probability of assured forwarding services in DiffServ interior nodes under the processor sharing scheduling discipline. In *Proc. IEEE International Conference on Performance, Computing, and Communications*, pages 223–230.

Blake, S., Black, D., Carlson, M., Davies, E., Wang, Z., and Weiss, W. (1998). An architecture for differentiated services. IETF RFC 2475.

Bonenfant, P. (1998). Optical layer survivability : a comprehensive approach. In *Proc. Optical Fiber Communication Conference*, pages 270–271.

Botta, A., Dainotti, A., and Pescape, A. (2007). Multi-protocol and multi-platform traffic generation and measurement. INFOCOM 2007 DEMO Session.

Bouras, C. and Sevasti, A. (2003). Analytical approach and verification of a DiffServ-based priority service. In *Proc. IEEE International Conference on High Speed Networks and Multimedia Communications*, pages 11–20.

Braden, R., Clark, D., and Shenker, S. (1994). RFC 1633 : Integrated services in the Internet architecture : an overview. IETF.

Chen, B. and Wang, J. (2003). Hybrid switching and P-routing for optical burst switching network. *IEEE Journal on Selected Areas in Communications*, **21**(7), 1071–1080.

Chim, T. W., Yeung, K., and Lui, K.-S. (2005). Traffic distribution over equal-cost-multi-paths. *Computer Networks*, **49**(4), 465–75.

Crochat, O. and LeBoudec, J.-Y. (1998). Design protection for WDM optical networks. *IEEE Journal on Selected Areas in Communications*, **16**(7), 1158–1165.

Crochat, O., LeBoudec, J.-Y., and Gerstel, O. (2000). Protection interoperability for WDM optical networks. *IEEE/ACM Transactions on Networking*, **8**(3), 384–395.

El-Gendy, M. A., Bose, A., Wang, H., and Shin, K. G. (2003). Statistical characterization for per-hop QoS. In *Proc. IEEE International Workshop on Quality of Service*, pages 21–40.

Faucheur, F. L. (2005a). Maximum allocation bandwidth constraints model for diffserv-aware mpls traffic engineering. IETF RFC 4125 (Experimental).

Faucheur, F. L. (2005b). Russian dolls bandwidth constraints model for diffserv-aware mpls traffic engineering. IETF RFC 4127 (Experimental).

Faucheur, F. L. and Lai, W. (2003). RFC 3564 : Requirements for support of differentiated services-aware MPLS traffic engineering. IETF.

Faucheur, F. L., Wu, L., Davie, B., Davari, S., Vaananen, P., Krishnan, R., Cheval, P., and Heinanen, J. (2002). RFC 3270 : Multi-protocol label switching (MPLS) support of differentiated services. IETF.

Feng, B., Bhatnagar, A., and etc., K. O. (2003). Scalable optical IP transport networks (SCORPION). Technical information, Eurescom.

Ferrari, T. and Chimento, P. (2000). A measurement-based analysis of expedited forwarding PHB mechanisms. *Proc. Eighth International Workshop on Quality of Service*, pages 127–137.

Filsfils, C. and Evans, J. (2002). Engineering a multiservice IP backbone to support tight SLAs. *Computer Networks*, **40**(1), 131–148.

Fumagalli, A. and Tacca, M. (2001). Differentiated reliability (DiR) in WDM rings without wavelength converters. *ICC 2001. IEEE International Conference on Communications. Conference Record (Cat. No.01CH37240)*, **9**, 2887 – 91.

Fumagalli, A., Tacca, M., Unghvary, F., and Farago, A. (2002). Shared path protection with differentiated reliability. *2002 IEEE International Conference on Communications. Conference Proceedings. ICC 2002 (Cat. No.02CH37333)*, **4**, 2157 – 61.

Fumagalli, A. and Valcarenghi, L. (2000). IP restoration vs. WDM protection : is there an optimal choice ? *IEEE Network*, **14**(6), 34–41.

Gerstel, O. and Ramaswami, R. (2000a). Optical layer survivability—an implementation perspective. *IEEE Journal on Selected Areas in Communications*, **18**(10), 1885–1899.

Gerstel, O. and Ramaswami, R. (2000b). Optical layer survivability : a services perspective. *IEEE Communications Magazine*, **38**(3), 104–113.

Gerstel, O. and Sasaki, G. (2001). Quality of protection (QoP) : a quantitative unifying paradigm to protection service grades. *Proceedings of the SPIE — The International Society for Optical Engineering*, **4599**, 12–23.

Gowda, S. and Sivalingam, K. M. (2003). Protection mechanisms for optical WDM networks based on wavelength converter multiplexing and backup path relocation techniques. In *Proc. IEEE INFOCOM*, volume 1, pages 12–21.

Heinanen, J., Baker, F., Weiss, W., and Wroclawski, J. (1999). Assured forwarding PHB group. IETF RFC 2597.

Heinanen, J. and Guerin, R. (1999a). RFC 2697 : A single rate three color marker. IETF.

Heinanen, J. and Guerin, R. (1999b). RFC 2698 : A two rate three color marker. IETF.

Hsu, C.-F., Liu, T.-L., and Huang, N.-F. (2002). Performance analysis of deflection routing in optical burst-switched networks. *Proc. IEEE INFOCOM*, **1**, 66–73.

IEEE (2000). Amendment to carrier sense multiple access with collision detection (csma/cd) access method and physical layer specifications Ů aggregation of multiple link segments. Standard IEEE 802.3ad-2000.

Jacobson, V., Nichols, K., and Poduri, K. (1999). An expedite forwarding PHB. IETF RFC 2598.

Kim, D.-G., Ryu, S.-W., Youn, J.-S., Youm, S.-K., Seok, S.-J., and Kang, C.-H. (2003). Multiple hierarchical protection schemes for differentiated services in GMPLS networks. In *Proc. International Conference on Information Technology : Research and Education*, pages 583 – 586.

Kimura, T., Kabashima, K., Aoki, M., and Urushidani, S. (2005). Proposal and comparison of QoS schemes for IP-over-optical multilayer networks. *IEICE Transactions on Communications*, **E88-B**(10), 3895–3903.

Kompella, K., Rekhter, Y., and Berger, L. (2005). RFC 4201 : Link bundling in MPLS traffic engineering. IETF.

Kos, A., Klepec, B., and Tomazic, S. (2002). Techniques for performance improvement of VoIP applications. In *Proc. 11th IEEE Mediterranean Electrotechnical Conference*, pages 250–254.

Koucheryavy, Y., Moltchanov, D., and Harju, J. (2003). A top-down approach to VoD traffic transmission over DiffServ domain using AF PHB class. In *Proc. ICC 2003 — IEEE International Conference on Communications*, volume 26, pages 243–249.

Kurant, M. and Thiran, P. (2005). On survivable routing of mesh topologies in IP-over-WDM networks. *Proc. IEEE INFOCOM*, **2**, 1106–1116.

Lee, H.-I. (2006). A two-stage switch with load balancing scheme maintaining packet sequence. *IEEE Communications Letters*, **10**(4), 290–292.

Lee, J., Lee, K.-H., Lee, J. H., Hahm, J. H., and Kim, Y. S. (2003). Design and analysis of MPLS-based ATM switching system for differentiated services. In *Eighth IEEE International Symposium on Computers and Communication*, pages 969–974.

Limal, E., Danielsen, S., and Stubkjaer, K. (1998). Capacity utilization in resilient wavelength-routed optical networks using link restoration. In *Proc. Optical Fiber Communication Conference and Exhibit*, Technical Digest, pages 297–298. OSA.

Maier, G., Pattavina, A., Patre, S. D., and Martinelli, M. (2002). Optical network survivability : Protection techniques in the WDM layer. *Photonic Network Communications*, **4**(3), 251–269.

Mannie, E. and Papadimitriou, D. (2004). Recovery (protection and restoration) terminology for generalized multi-protocol label switching (GMPLS). IETF.

Matrawy, A., Lambadaris, I., and Huang, C. (2002). MPEG4 traffic modeling using the transform expand sample methodology. In *Proceedings of 4th IEEE International Workshop on Network Appliances*, Gaithersburg, Maryland.

May, M., Bolot, J.-C., Jean-Marie, A., and Diot, C. (1999). Simple performance models of differentiated services schemes for the Internet. In *Proc. IEEE INFOCOM'99*, pages 1385–1395.

Medard, M., Finn, S. G., Barry, R. A., and Gallager, R. G. (1999). Redundant trees for preplanned recovery in arbitrary vertex-redundant or edge-redundant graphs. *IEEE/ACM Transactions on Networking*, **7**(5), 641–652.

Metz, C. (2000). IP protection and restoration. *IEEE Internet Computing*, **4**(2), 97–102.

Mills, D. (1992). Network time protocol (version 3) specification, implementation. IETF RFC 1305.

Minei, I. (2004). MPLS DiffServ-aware traffic engineering. White paper, Juniper Networks.

Ming, C., Zhou, L., and Gurusamy, M. (2005). Dynamic routing of dependable connections with different QoP grades in WDM optical networks. In *Proc. IEEE Symposium on Computers and Communications*, pages 532–537.

Modiano, E. and Narula-Tam, A. (2002). Survivable lightpath routing : A new approach to the design of WDM-based networks. *IEEE Journal on Selected Areas in Communications*, **20**(4), 800–809.

Naser, H. and Mouftah, H. (2004). A multilayer differentiated protection services architecture. *IEEE Journal on Selected Areas in Communications*, **22**(8), 1539–1547.

Nguyen, L., Eyers, T., and Chicharo, J. (2000). Differentiated service performance analysis. In *Proceedings Fifth IEEE Symposium on Computers and Communications*, pages 328–333.

Nichols, K., Jacobson, V., and Zhang, L. (1999). RFC 2638 : A two-bit differentiated services architecture for the internet. IETF.

Papadimitriou, G. I., Papazoglou, C., and Pomportsis, A. S. (2003). Optical switching : Switch fabrics, techniques and architectures. *Journal of Lightwave Technology*, **21**(2), 384–405.

Patek, S., Venkateswaran, R., and Liebeherr, J. (2001). Simple alternate routing for differentiated services networks. *Computer Networks*, **37**(3-4), 447–466.

Pattavina, A. (2005). Performance of IP optical packet networks with deflection routing. In *Proc. IEEE International Conference on Communications*, volume 3, pages 1663–1667.

Pham, D.-L., Sugawara, S., and Miki, T. (2004). QoS differentiation resource allocation for assured service in differentiated services networks. *IEICE Transactions on Communications*, **E87-B**(7), 1984–1992.

Ramamurthy, S. and Mukherjee, B. (1999a). Survivable WDM mesh networks. ii. restoration. In *Proc. IEEE International Conference on Communications*, volume 3, pages 2023–2030.

Ramamurthy, S. and Mukherjee, B. (1999b). Survivable WDM mesh networks. part I-protection. In *Proc. IEEE INFOCOM*, volume 2, pages 744–751.

Ramamurthy, S., Sahasrabuddhe, L., and Mukherjee, B. (2003). Survivable WDM mesh networks. *Journal of Lightwave Technology*, **21**(4), 870–883.

Rosen, E., Viswanathan, A., and Callon, R. (2001). RFC 3031 : Multiprotocol label switching architecture. IETF.

Sahasrabuddhe, L., Ramamurthy, S., and Mukherjee, B. (2002). Fault management in IP-over-WDM networks : WDM protection versus IP restoration. *IEEE Journal on Selected Areas in Communications*, **20**(1), 21–33.

Sahu, S., Towsley, D., and Kurose, J. (1999). Quantitative study of differentiated services for the internet. In *Proc. IEEE Global Telecommunications Conference*, volume 3, pages 1808–1817.

Sansò, B., Awad, C., and Girard, A. (2006). Can DiffServ guarantee IP QoS under failures ? *IEEE Network*, **20**(4), 32–40.

Saradhi, C., Gurusamy, M., and Zhou, L. (2004). Differentiated QoS for survivable WDM optical networks. *IEEE Communications Magazine*, pages S8–S14.

Saradhi, C. and Murthy, C. (2002). Routing differentiated reliable connections in WDM optical networks. *Optical Networks Magazine*, **3**(3), 50–67.

Saradhi, C. V. and Murthy, C. S. R. (2004). Dynamic establishment of differentiated survivable lightpaths in WDM mesh networks. *Computer Communications*, **27**(3), 273–294.

Schneider, G. and Nemeth, T. (2002). A simulation study of the OSPF-OMP routing algorithm. *Computer Networks*, **39**(4), 457–468.

Semeria, C. and Stewart III, J. (2001). Supporting differentiated service classes in large IP networks. White paper, Juniper Networks.

Sengupta, S., Saha, D., and Chaudhuri, S. (2002). Analysis of enhanced OSPF for routing lightpaths in optical mesh networks. In *Proc. IEEE International Conference on Communications*, volume 5, pages 2865–2869.

Shi, W., MacGregor, M., and Gburzynski, P. (2005). Load balancing for parallel forwarding. *IEEE/ACM Transactions on Networking*, **13**(4), 790–801.

Sivalingam, K. M. and Subramaniam, S. (2000). *Optical WDM Networks : Principle and Practice.* Kluwer Academic Publishers.

Sivarajan, K. N. (2000). Optical networking systems—trends and opportunities. White paper, Tejas Networks.

Trimintzios, P., Bauge, T., Pavlou, G., Georgiadis, L., Egan, R., and Flegkas, P. (2002). Quality of service provisioning for supporting premium services in IP networks. In *Proc. IEEE Global Telecommunications Conference*, pages 2473–2477.

Vasseur, J.-P., Pickavet, M., and Demeester, P. (2004). *Network Recovery : Protection and Restoration of Optical, SONET-SDH, IP, and MPLS.* Morgan Kauffman.

Veerasamy, J., Venkatesan, S., and Shah, J. (1994). Effect of traffic splitting on link and path restoration planning. In *Proc. IEEE Global Telecommunications Conference*, volume 3, pages 1867–1871.

VideoLAN Project (2009). The VLC media player.

Vojnović, M. and Leboudec, J.-Y. (2002). Stochastic analysis of some expedited forwarding networks. In *Proceedings of IEEE INFOCOM*, volume 1, pages 1004–1013.

Wang, W., Liew, S., and Li, V. (2005). Solutions to performance problems in VoIP over a 802.11 wireless LAN. *IEEE Transactions on Vehicular Technology*, **54**(1), 366–384.

Widjaja, I. and Elwalid, A. (2003). Exploiting parallelism to boost data-path rate in high-speed IP/MPLS networking. In *Proc. IEEE INFOCOM*, volume 1, pages 566–575.

Wu, D. and Negi, R. (2003). Effective capacity : A wireless link model for support of quality of service. *IEEE Transactions on Wireless Communications*, **2**(4), 630–643.

Wu, K. and Reeves, D. (2003). Capacity planning of DiffServ networks with best-effort and expedited forwarding traffic. In *Proc. IEEE International Conference on Communications*, volume 3, pages 1902–1906.

Wu., K. and Reeves, D. (2004). Capacity planning of DiffServ networks with best-effort and expedited forwarding traffic. *Telecommunication Systems*, **25**(3-4), 193–207.

Wydrowski, B., Zukerman, M., Chuan, H. F., and Meini, B. (2002). Analytical performance evaluation of a two class DiffServ link. In *Proc. International Conference on Communication Systems*, volume 1, pages 373–377.

Xiang, B., Yu, H., Wang, S., and Li, L. (2004). A QoS-based differentiated protection algorithm in WDM mesh networks. In *Proc. International Conference on Communications, Circuits and Systems*, volume 1, pages 638–642.

Yao, W., Sahin, G., Li, M., and Ramamurthy, B. (2005). Analysis of multi-hop traffic grooming in WDM mesh networks. In *Proc. International Conference on Broadband Networks (Broadnets)*, volume 1, pages 165–174.

Ye, Y., Assi, C., Dixit, S., and Ali, M. (2001). A simple dynamic integrated provisioning/protection scheme in IP over WDM networks. *IEEE Communications Magazine*, **39**(11), 174–82.

Zarifzadeh, S., Khanmirza, H., and Yazdani, N. (2004). A multipath algorithm for premium traffic routing in DiffServ networks. In *Proc. 12th IEEE International Conference on Networks*, pages 572–577.

Zhang, H. and Durresi, A. (2002). Differentiated multi-layer survivability in IP/WDM networks. In *NOMS 2002 — IEEE/IFIP Network Operations and Management Symposium*, volume 8, pages 681–696.

Zhang, J. and Mukherjee, B. (2004). A review of fault management in WDM mesh networks : basic concepts and research challenges. *IEEE Network*, **18**(2), 41–48.

Zhou, D. and Subramaniam, S. (2000). Survivability in optical networks. *IEEE Network*, **14**(6), 16–23.

Ziviani, A., de Rezende, J., and Duarte, O. (1999). Towards a differentiated services support for voice traffic. In *Proc. IEEE Global Telecommunications Conference*, volume 1a, pages 59–63.

Ziviani, A., De Rezende, J. F., and Duarte, O. C. M. B. (2002). Evaluating the expedited forwarding of voice traffic in a differentiated services network. *International Journal of Communication Systems*, **15**(9), 799–813.

ANNEXE I

PARTAGE DE CHARGE ET DÉSORDRE DES PAQUETS

Les sections 1.2.1 montre l'existence et la popularité du *Link Bundling* au sein des réseaux IP sur WDM. Grâce à cette pratique, les capacités de transmission et les protocoles de routages des couches logiques deviennent plus extensibles et facilement adaptables aux besoins de débit de trafic toujours croissants. Le partage de charge est une conséquence directe du *Link Bundling* puisqu'un flot entre deux noeuds logiques est partagé sur plusieurs systèmes de transmission physique.

Le partage de charge peut se faire suivant deux méthodes, par paquet ou par flot. Dans le premier cas, deux paquets consécutifs d'un même flot peuvent suivre des chemins différents. Ceci est montré dans la partie supérieure de la figure I.1. Chaque paquet est transmis aléatoirement sur un des trois chemins disponibles. Le paquet 1 du flot carré est envoyé sur le plus court chemin, le paquet 2 sur le plus long chemin et le paquet 3 sur le chemin de longueur intermédiaire. Si le temps d'interarrivée entre les paquets 2 et 3 est très grand par rapport à la différence de délai entre les chemins quíls suivent, le paquet 2 aura le temps d'arriver à destination, sinon le paquet 3 arrivera avant le paquet 2, il y aura ainsi un désordre au niveau de l'arrivée des paquets à la destination. Le partage de charge par paquet permet cependant d'obtenir une utilisation de ressource proche d'être optimale mais peut causer un désordre relativement sévère dans l'arrivée des paquets à destination.

Le partage de charge peut également se faire par flot (*hashing*). S'il existe plusieurs flots de données entre une source et une destination, le réseau se charge de diviser le routage de ses flots entre les divers chemins possibles. Considérons le cas de la partie inférieure de la figure I.1. Deux flots $(1, 2, 3)$ et (a, b, c) existent entre la source et la destination. Le flot $(1, 2, 3)$ est transmis aléatoirement sur un des trois chemins, dans ce cas le plus court,

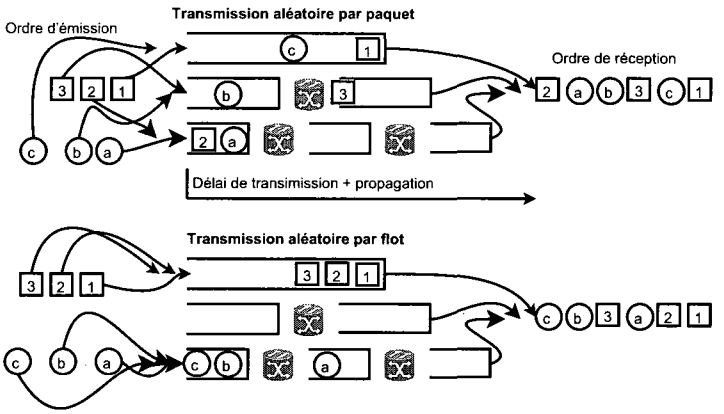


FIG. I.1 Deux mécanismes de partage de charge

le flot (a, b, c) est transmis sur le plus long. Cette méthode de partage de charge améliore grandement l'ordonnancement des paquets qui arrivent à destination mais résulte en un partage de charge sous-optimal. Plusieurs études (Chim et al., 2005), (Lee, 2006), (Yao et al., 2005) et (Shi et al., 2005) ont été réalisée dans le but de trouver une solution qui optimise l'équilibrage de charge entre plusieurs chemins candidats tout en minimisant le plus possible le désordre des paquets à l'arrivée. Les études prouvent sans équivoque que le partage de charge par flot reste meilleur puisqu'il est capable de garantir une livraison ordonnée des paquets à destination. Cette technique est celle retenue dans le cas des réseaux (G)MPLS/WDM dans lesquels le partage de charge se fait par LSP.

I.1 Partage de charge dans le modèle DiffServ*

Le modèle DiffServ* exige un partage de charge équilibré du trafic IP sur plusieurs canaux optiques. Dans le cas où les canaux optiques suivent des chemins disjoints, leur délai de bout-en-bout peut varier. Si DiffServ* est déployé au sein d'un réseau MPLS/WDM, aucun problème de désordre des paquets n'existera puisque le partage se fera par LSP donc par flot.

Un partage de charge par paquet serait idéal dans le cas de DiffServ*, puisqu'il lui permet de réagir le plus rapidement possible en cas de panne d'un des systèmes de transmission. Rappelons que dans le cas de DiffServ*, la panne d'un des trois systèmes de transmission, cause la réduction immédiate du débit du serveur DiffServ*. Les paquets servis en priorité par ce serveur, seront immédiatement distribués entre les systèmes de transmission fonctionnels restants. Si le partage de charge était par flot, le modèle DiffServ* devrait non seulement réduire son débit mais rerouter les flots affectés par la panne sur un des liens de transmissions restants (cf. section 4.3.6).

Dans le cas où le partage de charge doit absolument se faire par paquet, un problème de désordre des paquets peut survenir. Cette section montre que le désordre des paquets ne cause pas une dégradation de QoS dans le cas de certaines applications prioritaires, par exemple, de voix sur IP (VoIP). Dans le cas où le désordre cause des problèmes non tolérables, la section I.2 montrent plusieurs solutions *DiffServ** qui permettent de le réduire.

Il est important de noter que la sévérité du désordre dépend de la différence entre la variation des délais des chemins et celle de l'interarrivée des paquets. Dans le cas d'un *Link Bundling* entre la couche IP et celle WDM, la variation de délai entre les différents chemins est déterministe puisqu'elle n'inclut que les délais de propagation et de transmission sur les canaux optiques. Il n'existe aucune attente au niveau transmission. Il est possible de comparer cette variation de délai déterministe au profil du trafic impliqué et de prédire le taux de désordre qui en résulte. Reste à étudier si le désordre et le réordonnancement des paquets à l'arrivée affectent grandement la qualité de service perçue par l'application. Pour répondre à cette question considérons le cas suivant.

Le modèle DiffServ* nécessite trois canaux optiques disjoints entre chaque paire de routeurs IP adjacents. Supposons le cas de la figure I.2. Trois paquets d'une même application doivent être transmis simultanément. La longueur de chaque chemin est définie par le délai de bout-en-bout subi par chaque paquet qui le traverse. Ce délai tient compte uniquement

des délais déterministes de propagation et de transmission des paquets. Nous supposons en plus que les trois chemins ont même capacité et les paquets sont de longueur fixe.

À $t = 0ms$, les paquets sont transmis de façon aléatoire. Le paquet 2 est envoyé sur le chemin de $40ms$, 3 sur celui de $60ms$ et 1 sur celui de $80ms$. À $t = 40ms$, la paquet 2 arrive à destination. Comme cette dernière attend le paquet 1, 2 est mis en attente parce qu'il n'est pas arrivé en séquence, elle considère qu'il est arrivé trop tôt. À $t = 60ms$, le paquet 3 arrive, il est mis en file derrière le paquet 2. Finalement à $t = 80ms$, le premier paquet arrive, il est immédiatement transmis vers la couche application, les paquets 2 et 3 sont maintenant en séquence (le paquet 1 étant déjà reçu) ils sont transmis directement après. Le paquet 2 a eu un délai de $80ms$ au lieu de $40ms$, le paquet 3 a subit un délai de $80ms$ au lieu de $60ms$

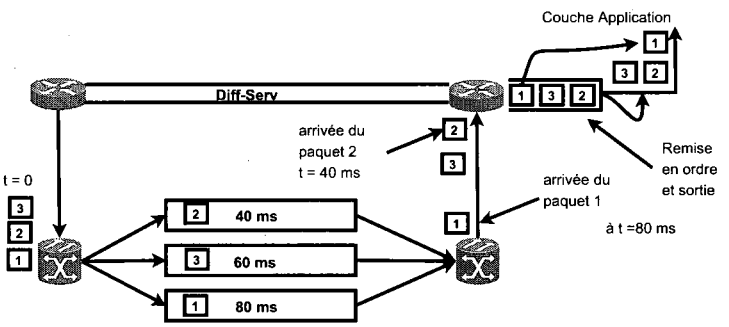


FIG. I.2 Processus de réordonnancement avec le modèle DiffServ*.

Selon (Kos et al., 2002), les tampons (*Jitter Buffer*) responsables de normaliser la gigue des paquets de voix sont déjà capables de réordonner ces paquets. Le réordonnancement se fait selon le numéro de séquence dans l'entête *Real Time Protocol* (RTP) du paquet. Supposons que l'application en question est une application de voix et qu'elle tolère un délai par paquet maximal de $100ms$. Les trois paquets 1,2 et 3 sont finalement reçus en ordre et à l'intérieur de la limite de délai permise. Si le délai de bout-en-bout des trois chemins respecte le niveau de QoS permis par l'application, aucun effet négatif sur la QoS ne sera observé. Si le délai du troisième chemin était de $120ms$, donc supérieur à $100ms$, les paquets 2 et 3 qui attendent l'arrivée du paquet 1 seront transmis vers l'application à

$t = 100ms$, le paquet 1 est considéré perdu, et sera rejeté à son arrivée.

Pour pallier à ce problème, plusieurs contraintes peuvent être imposée au modèle Diff-Serv*. L'une sera de limiter la transmission des paquets de voix (EF) au 2 plus courts chemins de façon à éviter le troisième chemin. Une autre option sera de mettre en place le modèle DiffServ* mais avec deux chemins physiques disjoints au lieu de trois. Une troisième option sera d'imposer l'utilisation de DiffProtect. Les paquets de voix (EF) sont tous transmis sur le plus court chemin. Les paquets des classes restantes (moins prioritaires) utiliseront les autres chemins.

I.2 Solutions *DiffServ** au problème de partage de charge par paquet

La raison pour laquelle le load sharing par paquet est conseillé dans le cas du modèle DiffServ* est qu'il garde le temps d'interruption de service à un strict minimum dans le cas d'une panne de canal optique. Le module de partage de charge par paquet n'a qu'à détecter la panne, éliminer un port de sortie de son processus de partage de charge aléatoire et aviser le serveur DiffServ* de réduire son débit. Alors que si le partage de charge se faisait par flot, il y aurait une certaine allocation flot-canal optique qui doit être redéfinie dans le cas d'une panne. Cette réallocation de flot semble plus longue.

Dans le cas où le désordre des paquets causé par le partage de charge par paquet affecte grandement la QoS perçue par l'application, plusieurs solutions peuvent être utilisées pour pallier à ce problème. La première sera de faire un partage de charge aléatoire par groupe de paquets. Ceci est montré dans la partie supérieure de la figure I.3. Dans ce cas le serveur DiffServ fonctionne avec la politique d'ordonnancement Weighted Round-Robin (WRR). Chaque file d'attente a un poids proportionnel à sa priorité. La file EF aura le plus grand poids, la file BE, le plus petit. Le poids détermine le taux de service de chaque file pendant une unité de temps. Plus le poids est élevé, plus le temps alloué au service de chaque file

est élevé, le nombre de paquets servis le sera aussi.

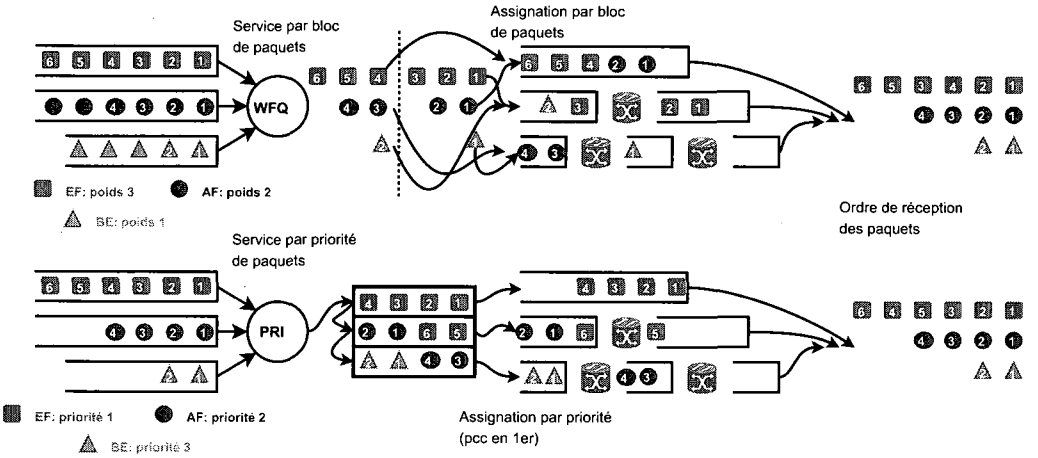


FIG. I.3 Partage de charge et DiffServ

Dans le cas de la figure I.3, 3 paquets EF, 2 paquets AF et 1 paquet BE sont servis pendant une unité de temps par l'ordonnanceur DiffServ. Les paquets servis doivent être transmis sur un des trois liens physiques disponibles. La transmission aléatoire peut se faire par paquet mais aussi par groupe de paquet. Ainsi la décision se fera par exemple, sur le groupe de 3 paquets EF. Ces paquets seront transmis en ordre sur un des trois chemins. Le groupe de paquets AF est suivant, le dernier sera le groupe de paquets BE. Au court de la prochaine unité de temps, une autre décision de transmission aléatoire sera faite sur le prochain groupe de paquet EF. Les résultats de simulation prouvent que cette option peut diminuer de façon considérable et parfois annuler le taux de désordre qui affecte chaque classe de paquet. Une configuration adéquate des poids de chaque classe en fonction du taux d'utilisation du serveur DiffServ (donc du lien IP) et de la différence de délai entre les chemins physiques peut rendre le taux de désordre nul. Le tableau I.1 résume quelques résultats de simulation obtenus.

La deuxième option est montrée dans la partie inférieure de la figure I.3. Elle est adaptée au cas où l'ordonnanceur DiffServ est de type prioritaire. Ce type d'ordonnancement sert les paquets par ordre de priorité. Seulement quand il n'y a plus de paquets EF à servir, les

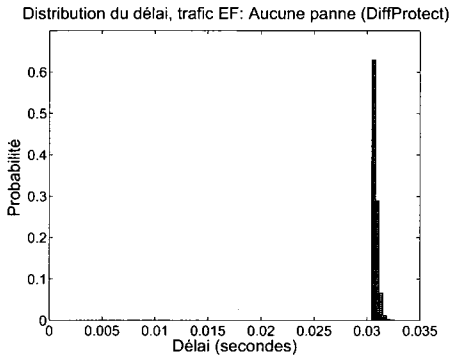
	Décision	**Taux d'utilisation du serveur WFQ de DiffServ** 100%	90%	80%	70%
Taux de désordre	par paquet	65%	45%	37%	31%
	par groupe	58%	15%	6%	0%

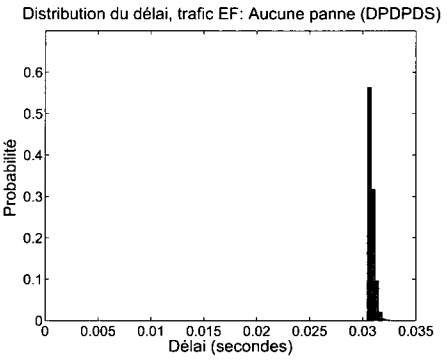
TAB. I.1 Performance de la décision aléatoire par groupe de paquets

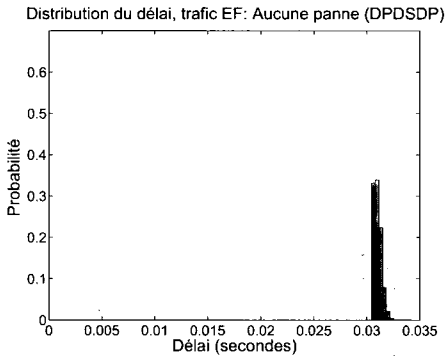
paquets AF sont servis. Les paquets BE sont les derniers à être considérés. La transmission sur les chemins physiques sera de type plus court chemin en premier. Les paquets EF sont les premiers à être servis, ils seront transmis sur le plus court chemin en premier. Si le débit des paquets EF est supérieur à la capacité du plus court chemin, les paquets EF restants sont transmis sur le deuxième PCC. Il en sera de même pour les paquets AF et BE. Cette méthode peut aussi diminuer le taux de désordre des paquets à l'arrivée.

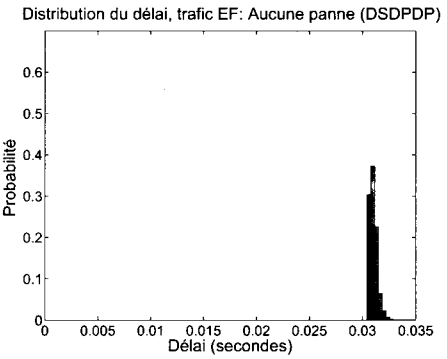
ANNEXE II

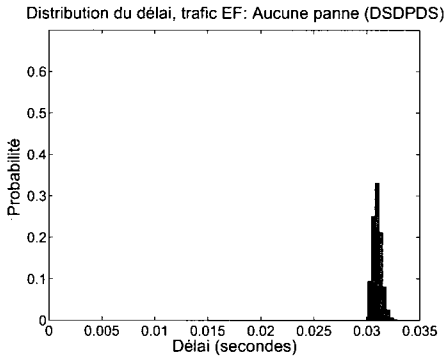
DISTRIBUTIONS DE DÉLAI ET GIGUE

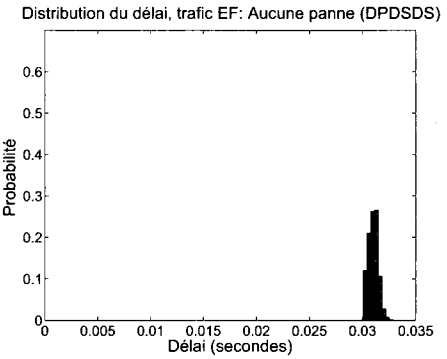

Distribution du délai, trafic EF: Aucune panne (DiffProtect)
Probabilité
Délai (secondes)

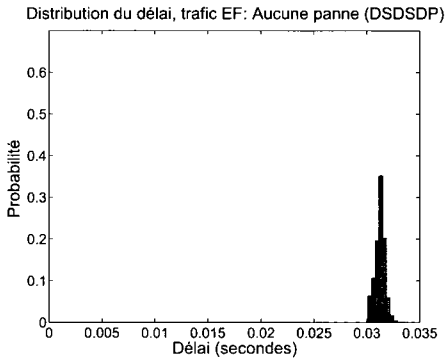

Distribution du délai, trafic EF: Aucune panne (DPDPDS)
Probabilité
Délai (secondes)

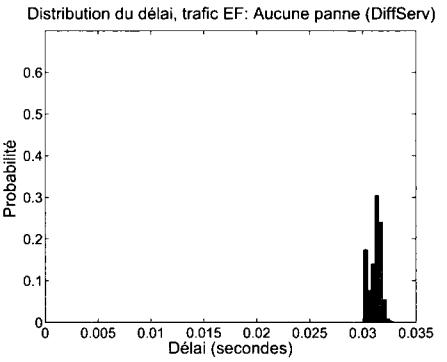

Distribution du délai, trafic EF: Aucune panne (DPDSDP)
Probabilité
Délai (secondes)

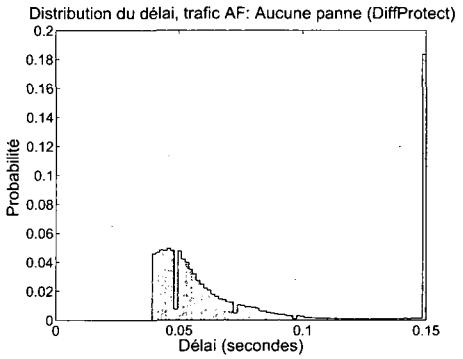

Distribution du délai, trafic EF: Aucune panne (DSDPDP)
Probabilité
Délai (secondes)

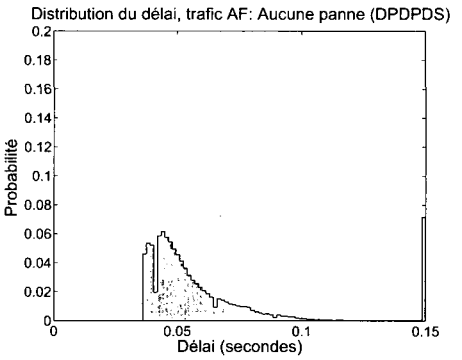

Distribution du délai, trafic EF: Aucune panne (DSDPDS)
Probabilité
Délai (secondes)

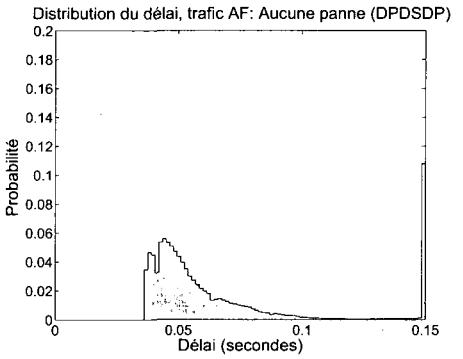

Distribution du délai, trafic EF: Aucune panne (DPDSDS)
Probabilité
Délai (secondes)

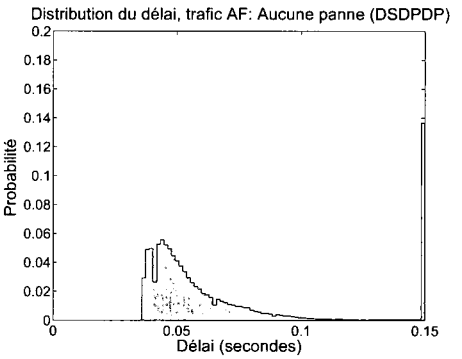

Distribution du délai, trafic EF: Aucune panne (DSDSDP)
Probabilité
Délai (secondes)

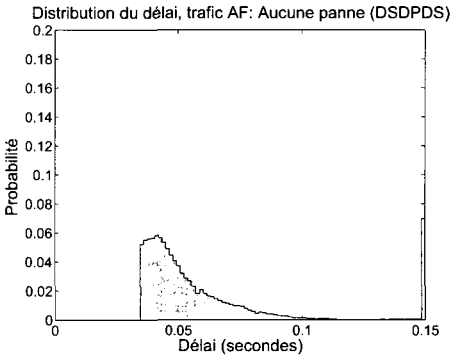

Distribution du délai, trafic EF: Aucune panne (DiffServ)
Probabilité
Délai (secondes)

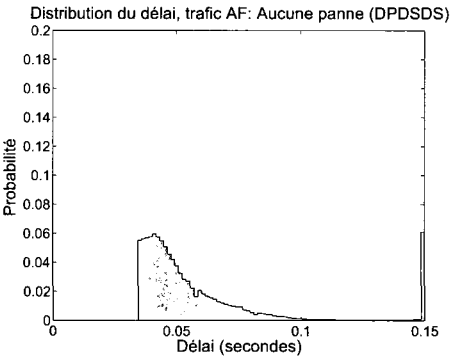

Distribution du délai, trafic AF: Aucune panne (DiffProtect)
Probabilité
Délai (secondes)

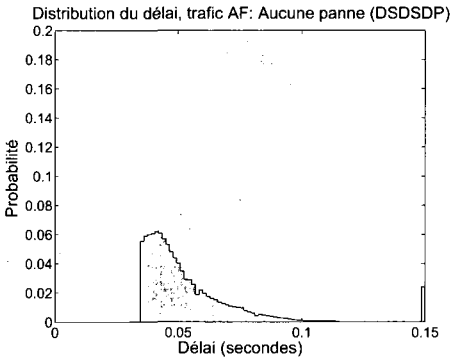

Distribution du délai, trafic AF: Aucune panne (DPDPDS)
Probabilité
Délai (secondes)

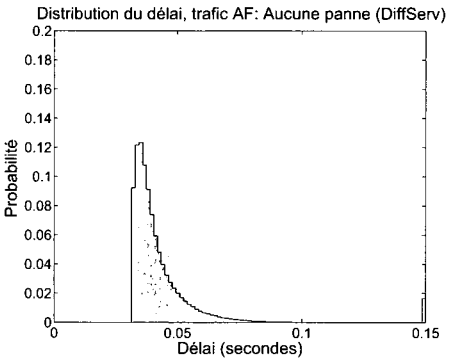

Distribution du délai, trafic AF: Aucune panne (DPDSDP)
Probabilité
Délai (secondes)

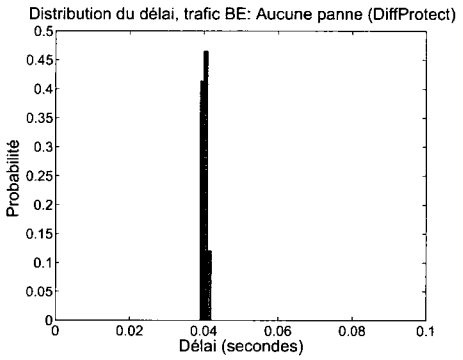

Distribution du délai, trafic AF: Aucune panne (DSDPDP)
Probabilité
Délai (secondes)

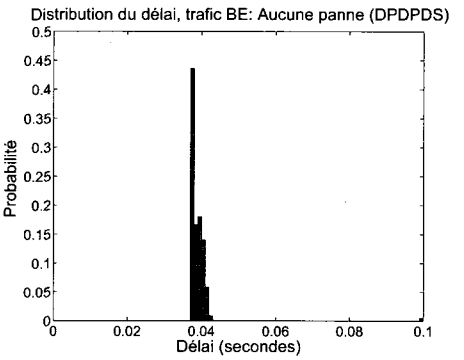

Distribution du délai, trafic AF: Aucune panne (DSDPDS)
Probabilité
Délai (secondes)

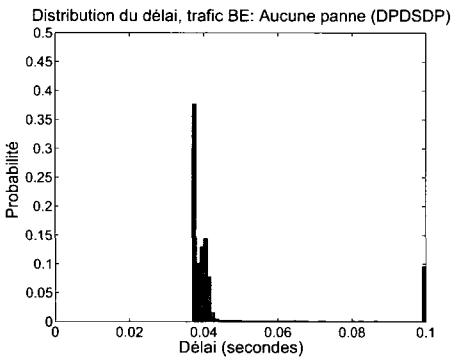

Distribution du délai, trafic AF: Aucune panne (DPDSDS)
Probabilité
Délai (secondes)

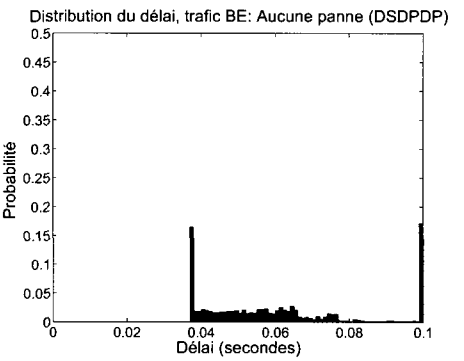

Distribution du délai, trafic AF: Aucune panne (DSDSDP)
Probabilité
Délai (secondes)

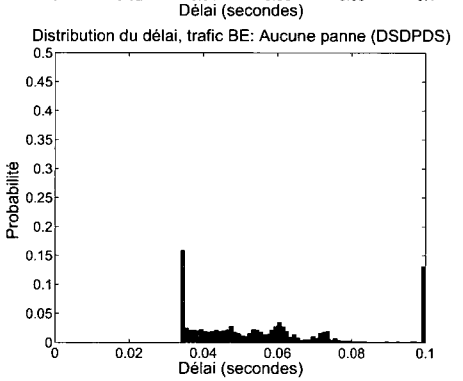

Distribution du délai, trafic AF: Aucune panne (DiffServ)
Probabilité
Délai (secondes)

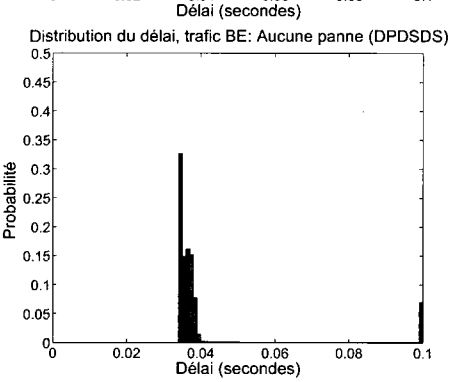

Distribution du délai, trafic BE: Aucune panne (DiffProtect)
Probabilité
Délai (secondes)

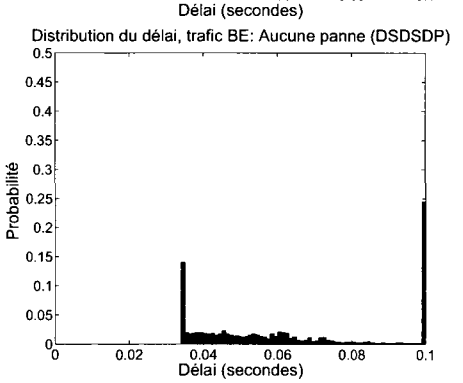

Distribution du délai, trafic BE: Aucune panne (DPDPDS)
Probabilité
Délai (secondes)

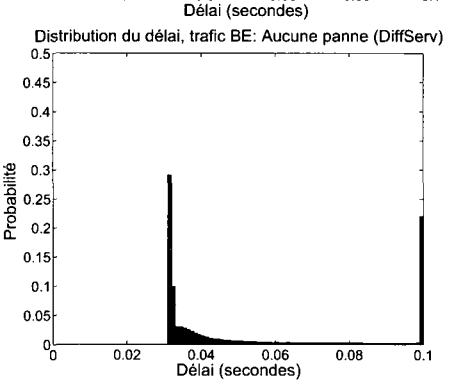

Distribution du délai, trafic BE: Aucune panne (DPDSDP)
Probabilité
Délai (secondes)

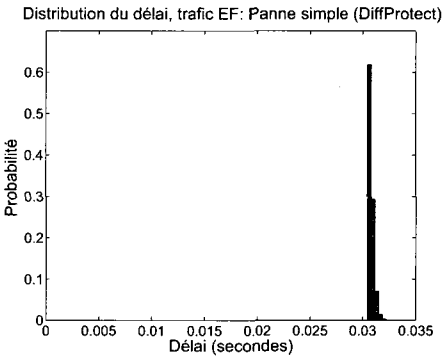

Distribution du délai, trafic BE: Aucune panne (DSDPDP)
Probabilité
Délai (secondes)

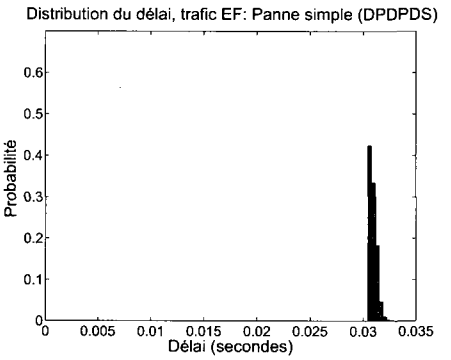

Distribution du délai, trafic BE: Aucune panne (DSDPDS)
Probabilité
Délai (secondes)

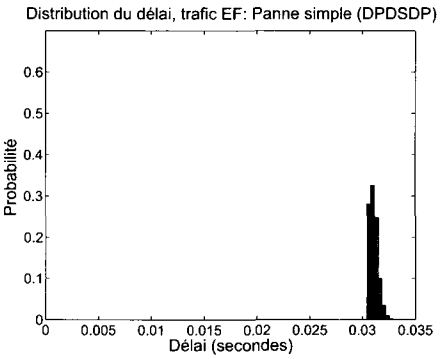

Distribution du délai, trafic BE: Aucune panne (DPDSDS)
Probabilité
Délai (secondes)

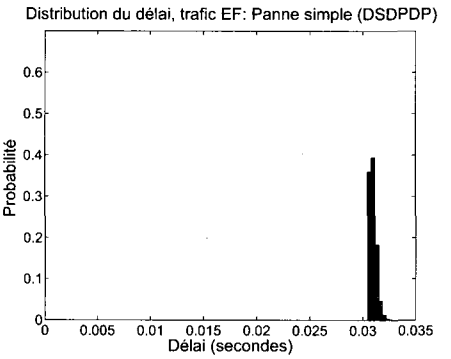

Distribution du délai, trafic BE: Aucune panne (DSDSDP)
Probabilité
Délai (secondes)

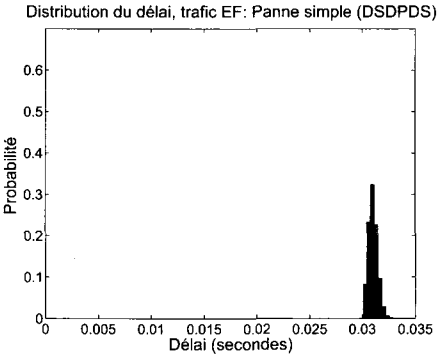

Distribution du délai, trafic BE: Aucune panne (DiffServ)
Probabilité
Délai (secondes)

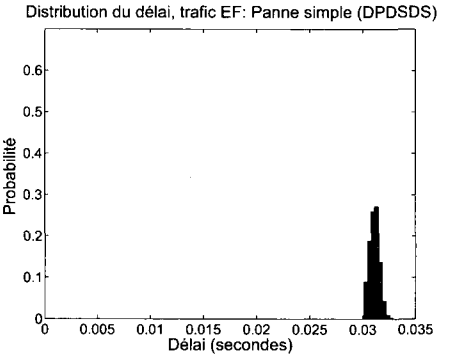

Distribution du délai, trafic EF: Panne simple (DiffProtect)
Probabilité
Délai (secondes)

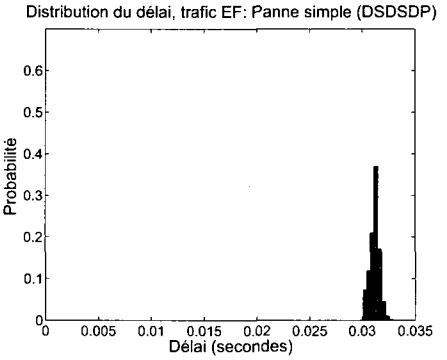

Distribution du délai, trafic EF: Panne simple (DPDPDS)
Probabilité
Délai (secondes)

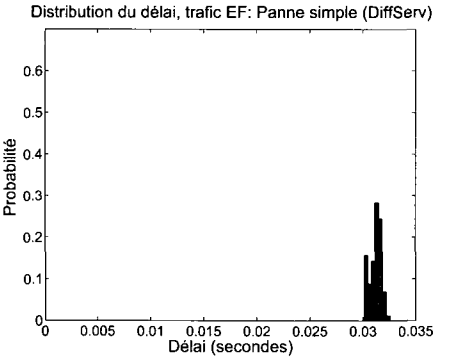

Distribution du délai, trafic EF: Panne simple (DPDSDP)
Probabilité
Délai (secondes)

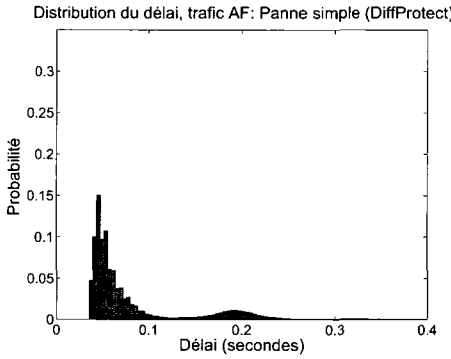

Distribution du délai, trafic EF: Panne simple (DSDPDP)
Probabilité
Délai (secondes)

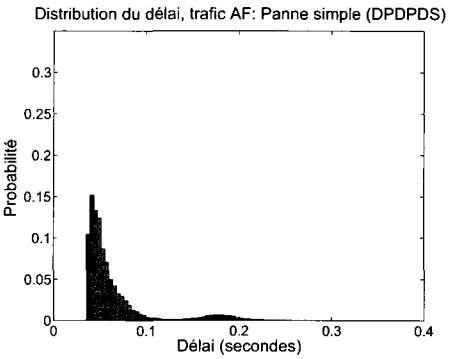

Distribution du délai, trafic EF: Panne simple (DSDPDS)
Probabilité
Délai (secondes)

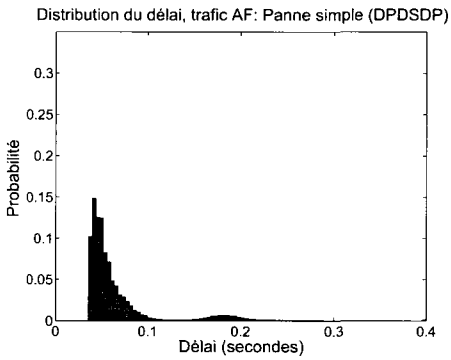

Distribution du délai, trafic EF: Panne simple (DPDSDS)
Probabilité
Délai (secondes)

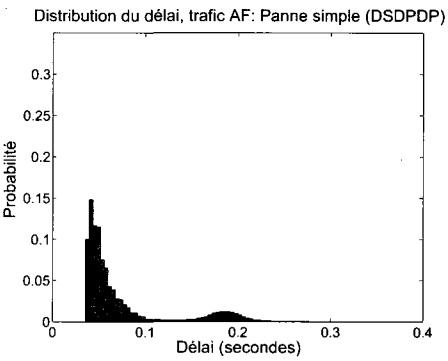

Distribution du délai, trafic EF: Panne simple (DSDSDP)
Probabilité
Délai (secondes)

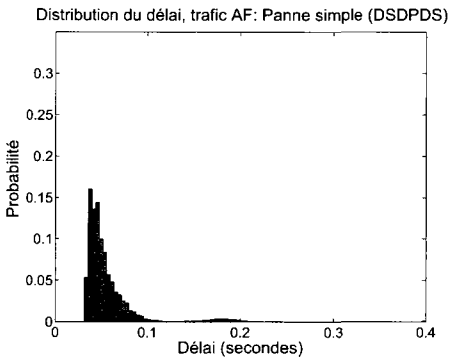

Distribution du délai, trafic EF: Panne simple (DiffServ)
Probabilité
Délai (secondes)

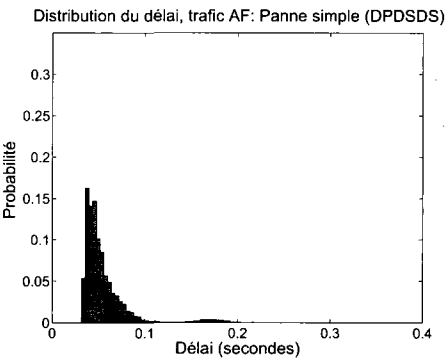

Distribution du délai, trafic AF: Panne simple (DiffProtect)
Probabilité
Délai (secondes)

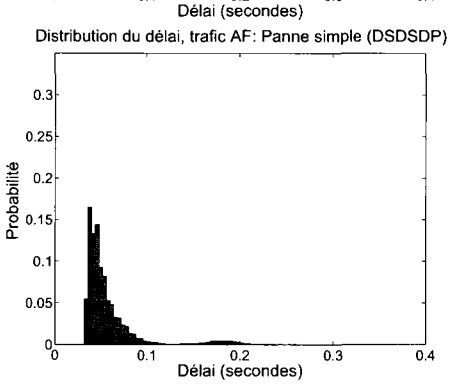

Distribution du délai, trafic AF: Panne simple (DPDPDS)
Probabilité
Délai (secondes)

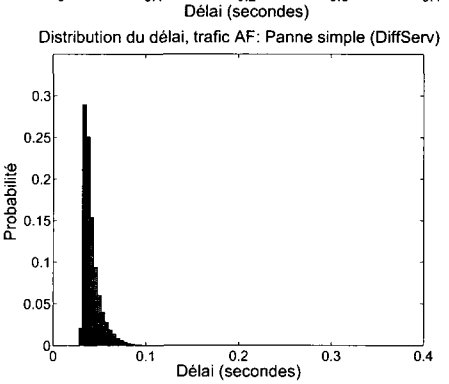

Distribution du délai, trafic AF: Panne simple (DPDSDP)
Probabilité
Délai (secondes)

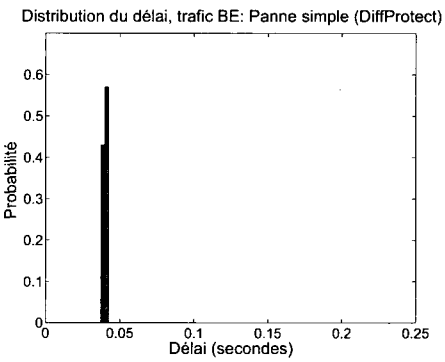

Distribution du délai, trafic AF: Panne simple (DSDPDP)
Probabilité
Délai (secondes)

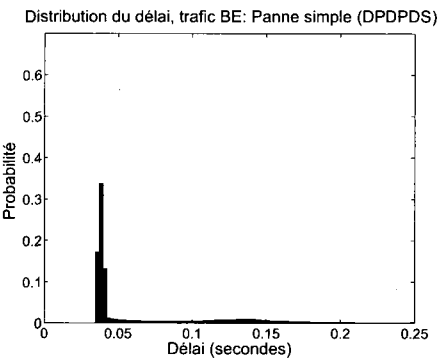

Distribution du délai, trafic AF: Panne simple (DSDPDS)
Probabilité
Délai (secondes)

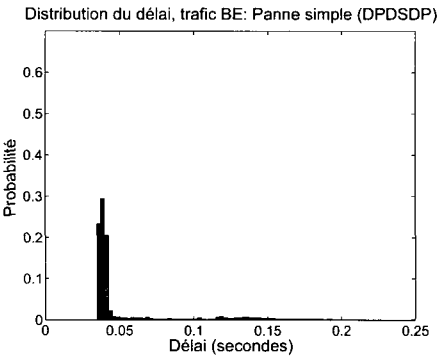

Distribution du délai, trafic AF: Panne simple (DPDSDS)
Probabilité
Délai (secondes)

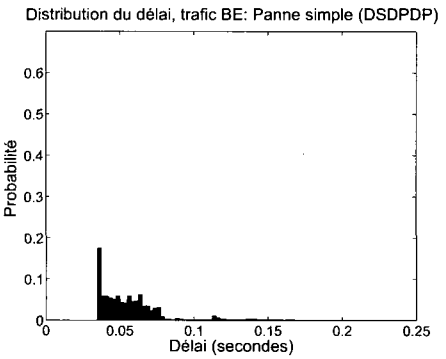

Distribution du délai, trafic AF: Panne simple (DSDSDP)
Probabilité
Délai (secondes)

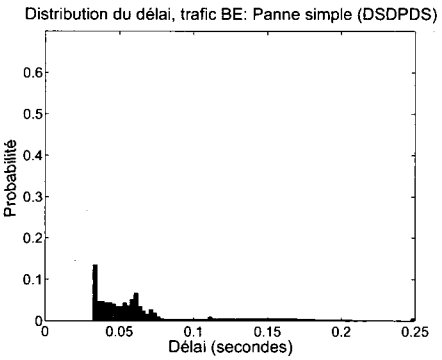

Distribution du délai, trafic AF: Panne simple (DiffServ)
Probabilité
Délai (secondes)

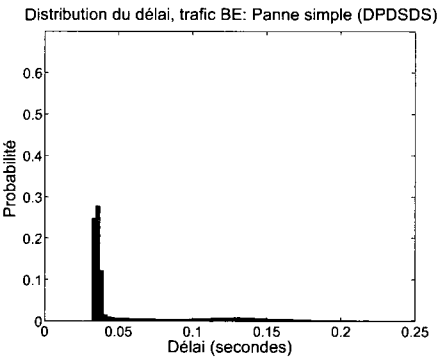

Distribution du délai, trafic BE: Panne simple (DiffProtect)
Probabilité
Délai (secondes)

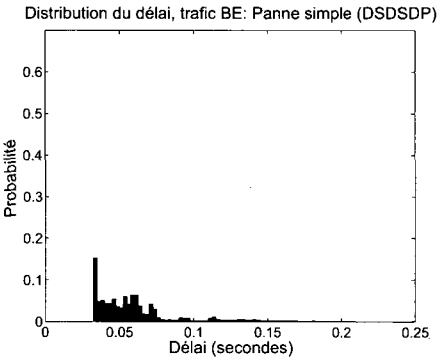

Distribution du délai, trafic BE: Panne simple (DPDPDS)
Probabilité
Délai (secondes)

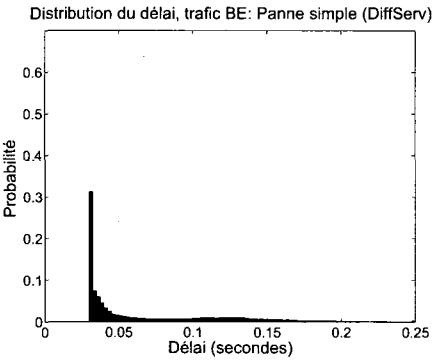

Distribution du délai, trafic BE: Panne simple (DPDSDP)
Probabilité
Délai (secondes)

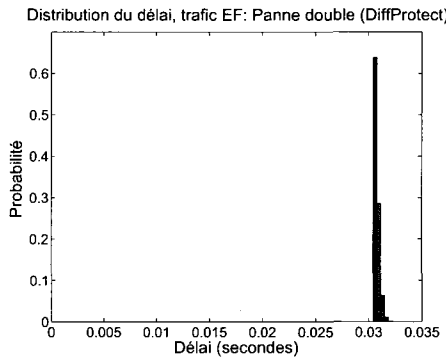

Distribution du délai, trafic BE: Panne simple (DSDPDP)
Probabilité
Délai (secondes)

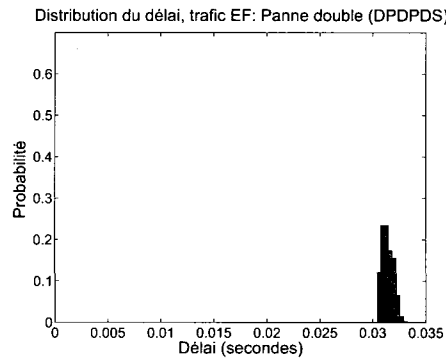

Distribution du délai, trafic BE: Panne simple (DSDPDS)
Probabilité
Délai (secondes)

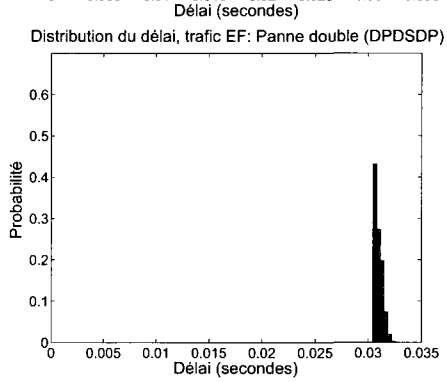

Distribution du délai, trafic BE: Panne simple (DPDSDS)
Probabilité
Délai (secondes)

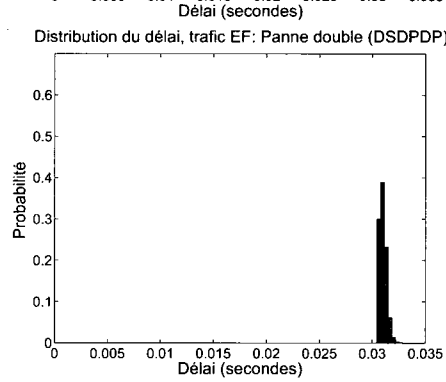

Distribution du délai, trafic BE: Panne simple (DSDSDP)
Probabilité
Délai (secondes)

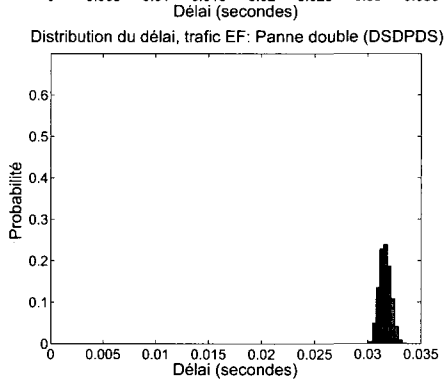

Distribution du délai, trafic BE: Panne simple (DiffServ)
Probabilité
Délai (secondes)

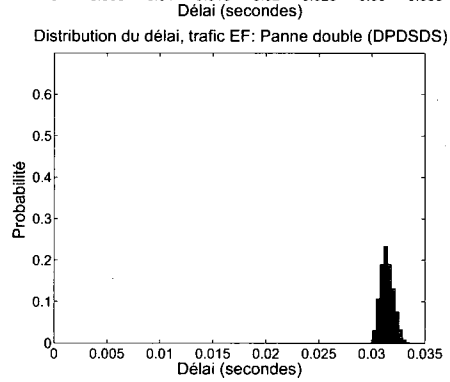

Distribution du délai, trafic EF: Panne double (DiffProtect)
Probabilité
Délai (secondes)

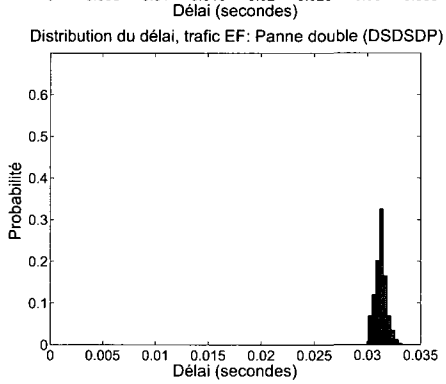

Distribution du délai, trafic EF: Panne double (DPDPDS)
Probabilité
Délai (secondes)

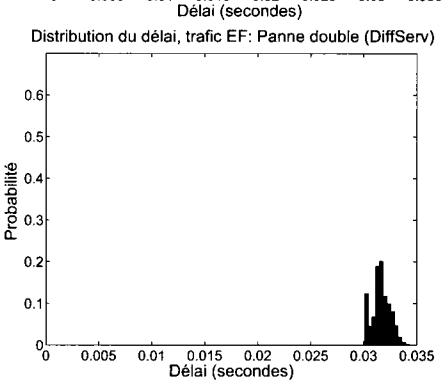

Distribution du délai, trafic EF: Panne double (DPDSDP)
Probabilité
Délai (secondes)

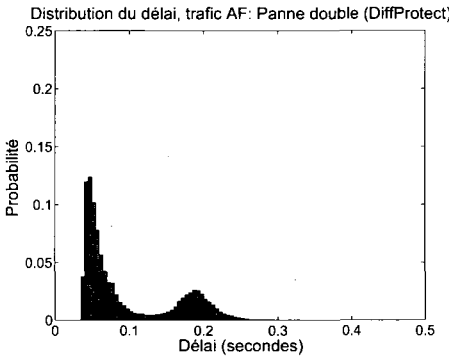

Distribution du délai, trafic EF: Panne double (DSDPDP)
Probabilité
Délai (secondes)

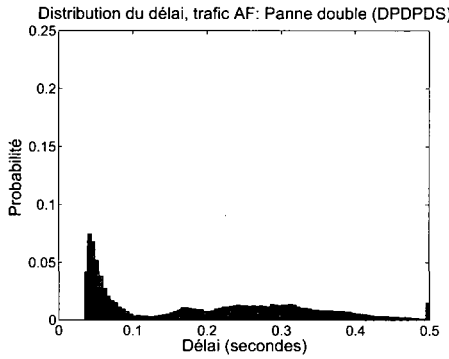

Distribution du délai, trafic EF: Panne double (DSDPDS)
Probabilité
Délai (secondes)

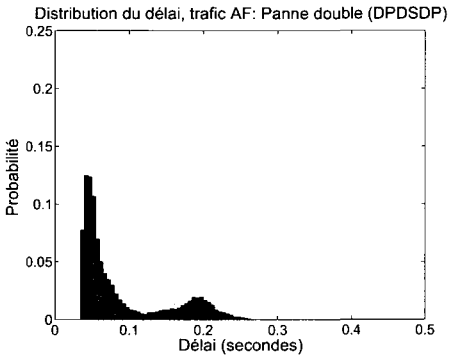

Distribution du délai, trafic EF: Panne double (DPDSDS)
Probabilité
Délai (secondes)

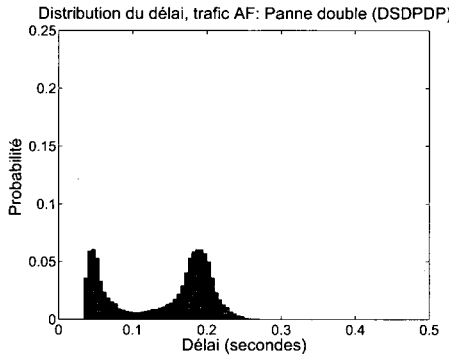

Distribution du délai, trafic EF: Panne double (DSDSDP)
Probabilité
Délai (secondes)

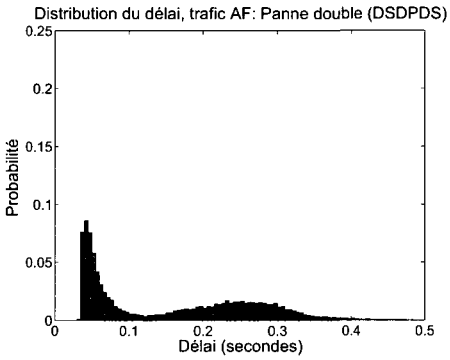

Distribution du délai, trafic EF: Panne double (DiffServ)
Probabilité
Délai (secondes)

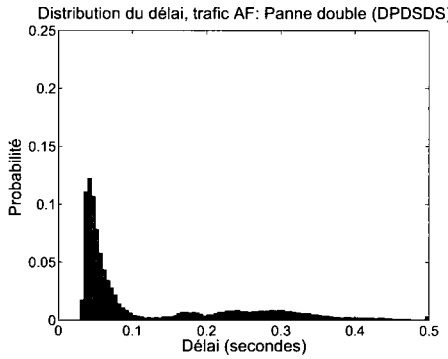

Distribution du délai, trafic AF: Panne double (DiffProtect)
Probabilité
Délai (secondes)

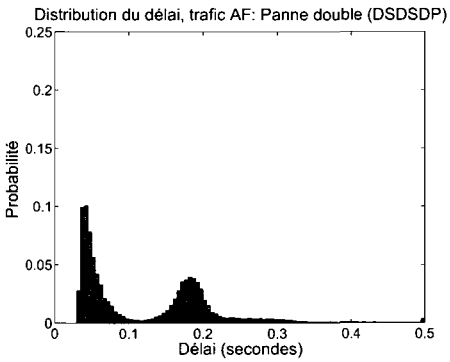

Distribution du délai, trafic AF: Panne double (DPDPDS)
Probabilité
Délai (secondes)

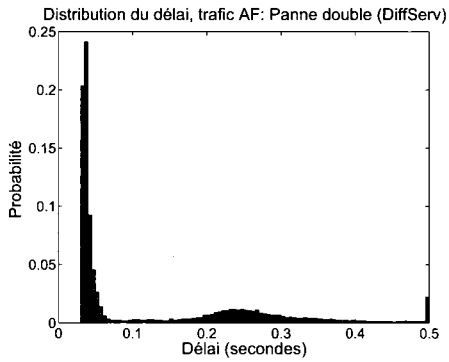

Distribution du délai, trafic AF: Panne double (DPDSDP)
Probabilité
Délai (secondes)

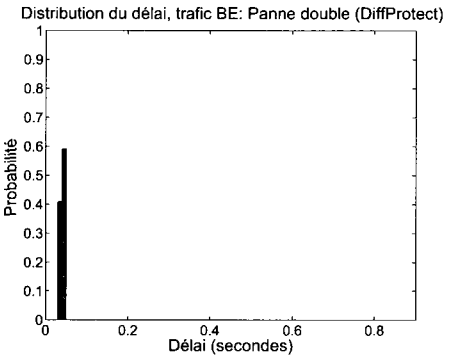

Distribution du délai, trafic AF: Panne double (DSDPDP)
Probabilité
Délai (secondes)

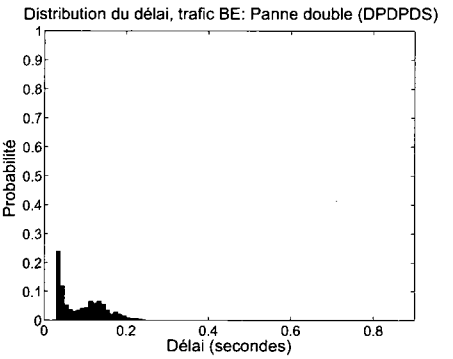

Distribution du délai, trafic AF: Panne double (DSDPDS)
Probabilité
Délai (secondes)

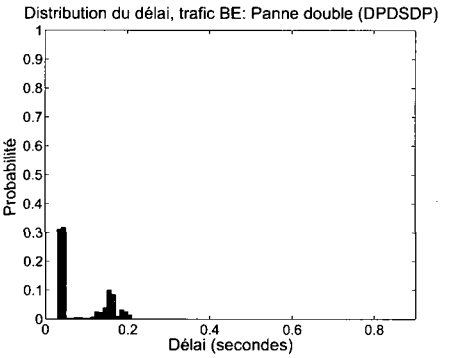

Distribution du délai, trafic AF: Panne double (DPDSDS)
Probabilité
Délai (secondes)

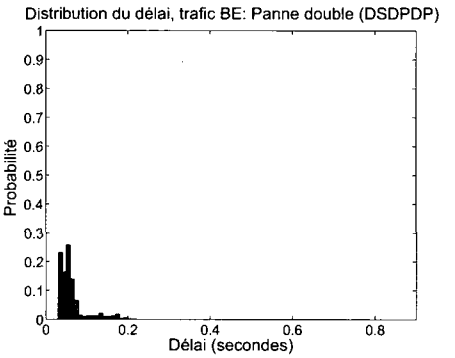

Distribution du délai, trafic AF: Panne double (DSDSDP)
Probabilité
Délai (secondes)

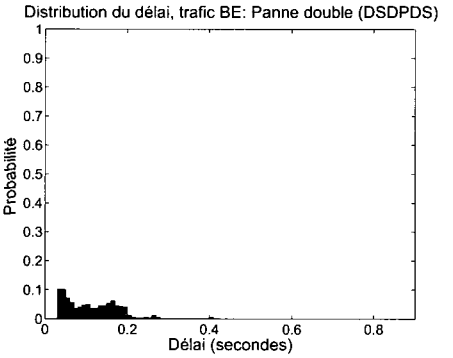

Distribution du délai, trafic AF: Panne double (DiffServ)
Probabilité
Délai (secondes)

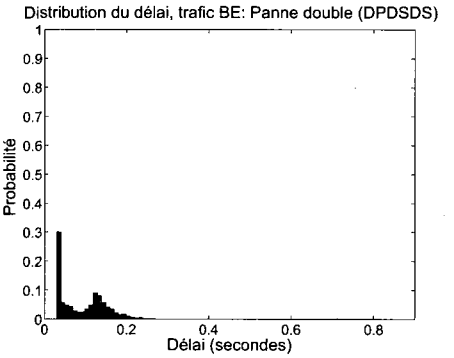

Distribution du délai, trafic BE: Panne double (DiffProtect)
Probabilité
Délai (secondes)

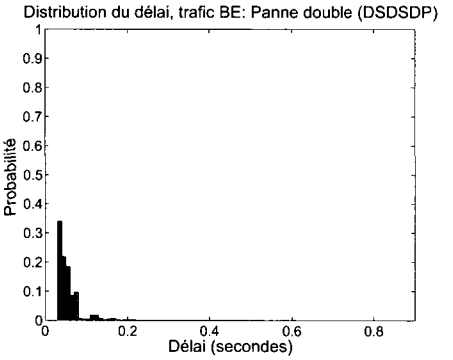

Distribution du délai, trafic BE: Panne double (DPDPDS)
Probabilité
Délai (secondes)

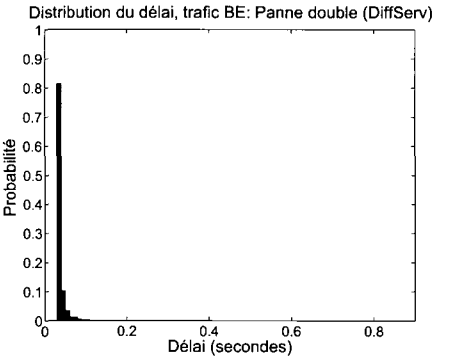

Distribution du délai, trafic BE: Panne double (DPDSDP)
Probabilité
Délai (secondes)

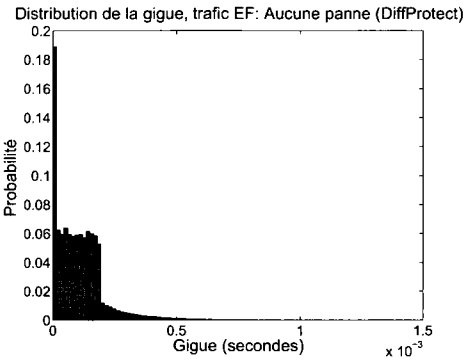

Distribution du délai, trafic BE: Panne double (DSDPDP)
Probabilité
Délai (secondes)

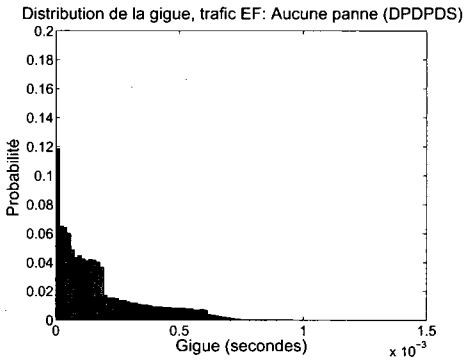

Distribution du délai, trafic BE: Panne double (DSDPDS)
Probabilité
Délai (secondes)

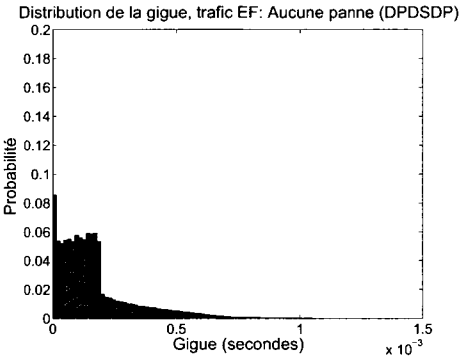

Distribution du délai, trafic BE: Panne double (DPDSDS)
Probabilité
Délai (secondes)

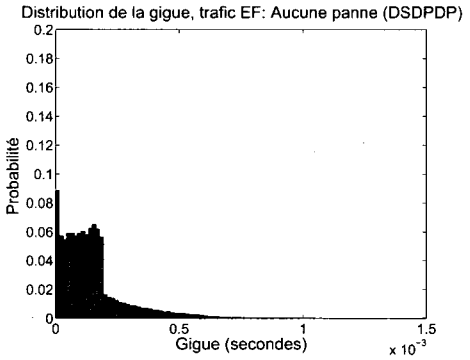

Distribution du délai, trafic BE: Panne double (DSDSDP)
Probabilité
Délai (secondes)

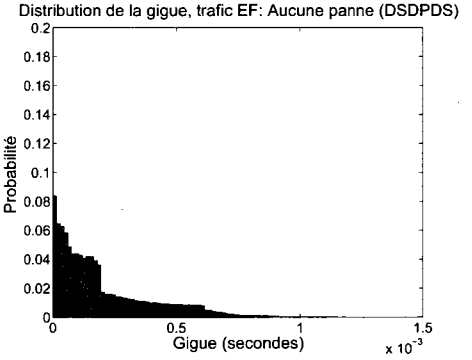

Distribution du délai, trafic BE: Panne double (DiffServ)
Probabilité
Délai (secondes)

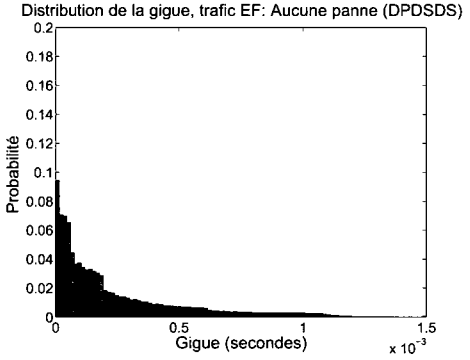

Distribution de la gigue, trafic EF: Aucune panne (DiffProtect)
Probabilité
Gigue (secondes)
x 10^-3

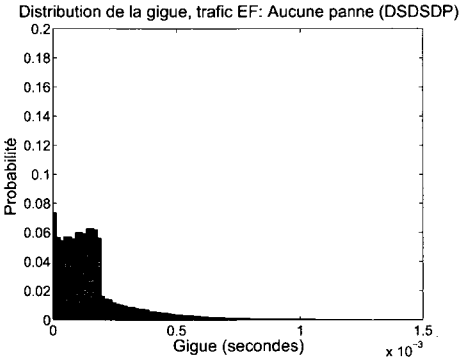

Distribution de la gigue, trafic EF: Aucune panne (DPDPDS)
Probabilité
Gigue (secondes)
x 10^-3

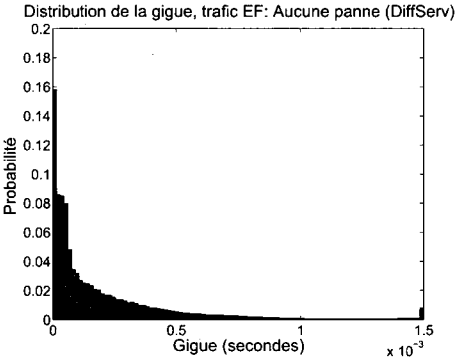

Distribution de la gigue, trafic EF: Aucune panne (DPDSDP)
Probabilité
Gigue (secondes)
x 10^-3

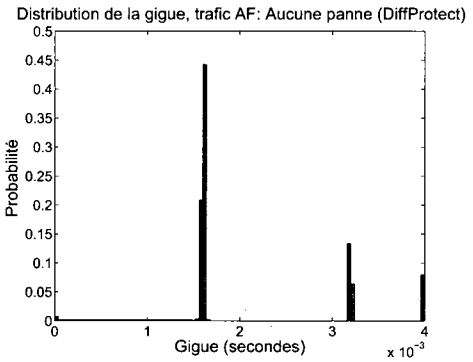

Distribution de la gigue, trafic EF: Aucune panne (DSDPDP)
Probabilité
Gigue (secondes)
x 10^-3

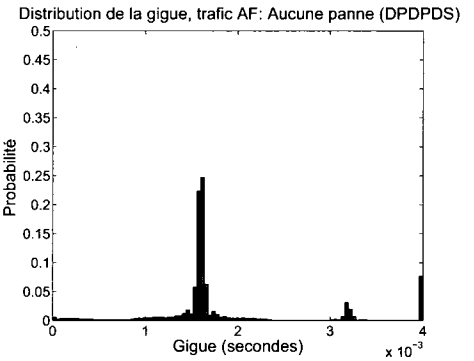

Distribution de la gigue, trafic EF: Aucune panne (DSDPDS)
Probabilité
Gigue (secondes)
x 10^-3

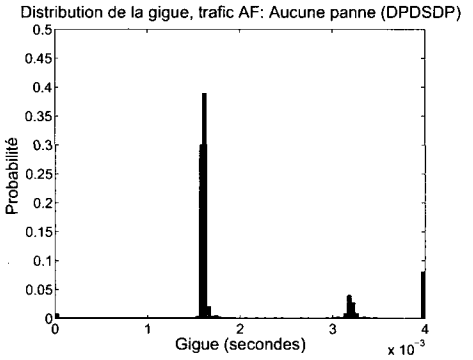

Distribution de la gigue, trafic EF: Aucune panne (DPDSDS)
Probabilité
Gigue (secondes)
x 10^-3

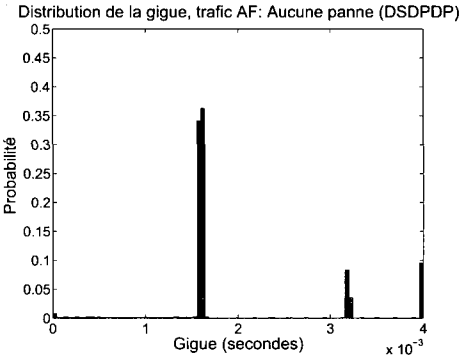

Distribution de la gigue, trafic EF: Aucune panne (DSDSDP)
Probabilité
Gigue (secondes)
x 10^-3

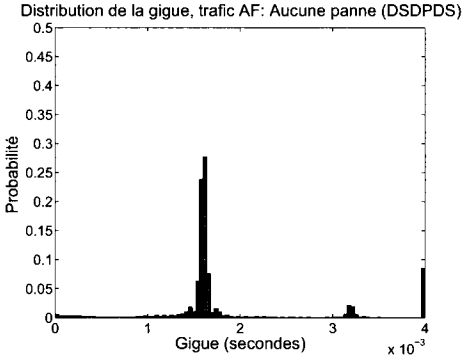

Distribution de la gigue, trafic EF: Aucune panne (DiffServ)
Probabilité
Gigue (secondes)
x 10^-3

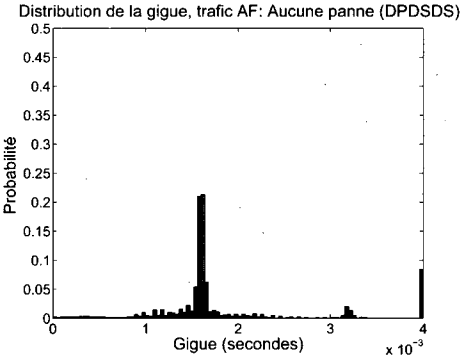

Distribution de la gigue, trafic AF: Aucune panne (DiffProtect)
Probabilité
Gigue (secondes)
x 10^-3

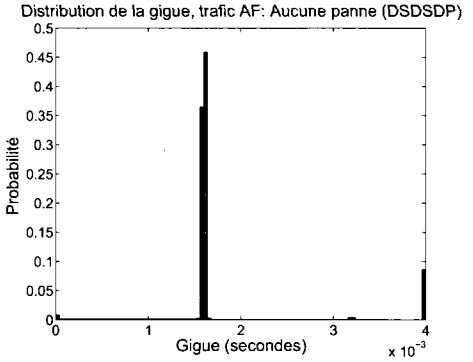

Distribution de la gigue, trafic AF: Aucune panne (DPDPDS)
Probabilité
Gigue (secondes)
x 10^-3

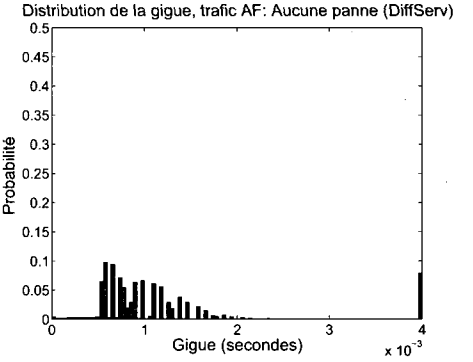

Distribution de la gigue, trafic AF: Aucune panne (DPDSDP)
Probabilité
Gigue (secondes)
x 10^-3

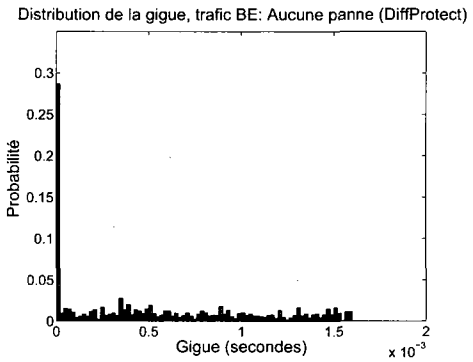

Distribution de la gigue, trafic AF: Aucune panne (DSDPDP)
Probabilité
Gigue (secondes)
x 10^-3

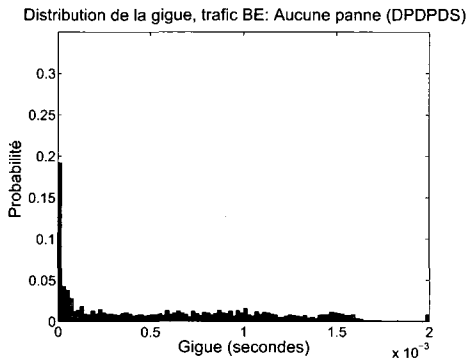

Distribution de la gigue, trafic AF: Aucune panne (DSDPDS)
Probabilité
Gigue (secondes)
x 10^-3

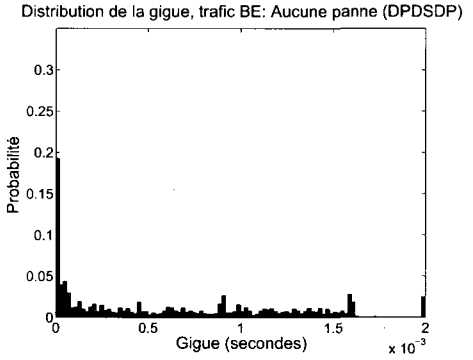

Distribution de la gigue, trafic AF: Aucune panne (DPDSDS)
Probabilité
Gigue (secondes)
x 10^-3

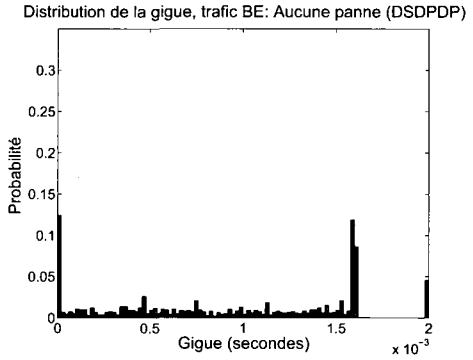

Distribution de la gigue, trafic AF: Aucune panne (DSDSDP)
Probabilité
Gigue (secondes)
x 10^-3

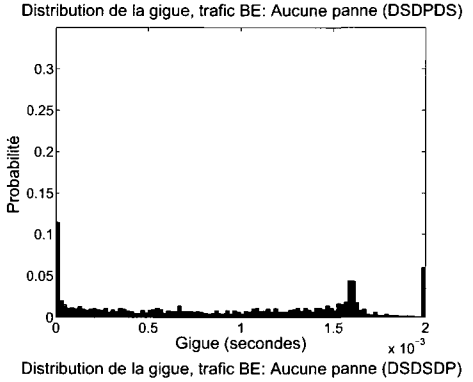

Distribution de la gigue, trafic AF: Aucune panne (DiffServ)
Probabilité
Gigue (secondes)
x 10^-3

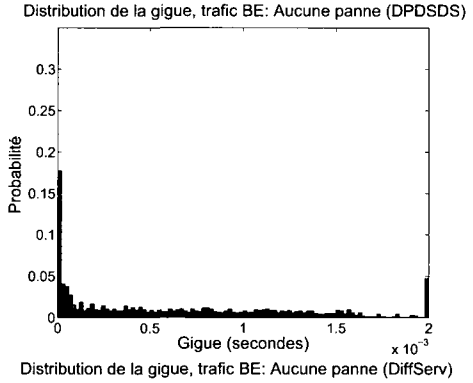

Distribution de la gigue, trafic BE: Aucune panne (DiffProtect)
Probabilité
Gigue (secondes)
x 10^-3

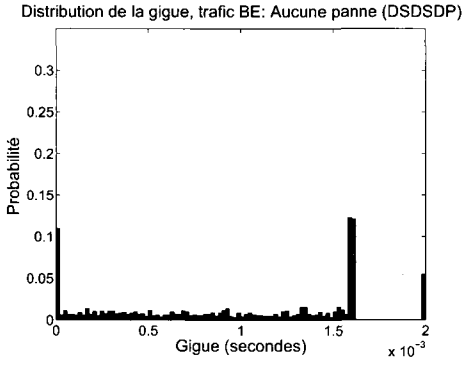

Distribution de la gigue, trafic BE: Aucune panne (DPDPDS)
Probabilité
Gigue (secondes)
x 10^-3

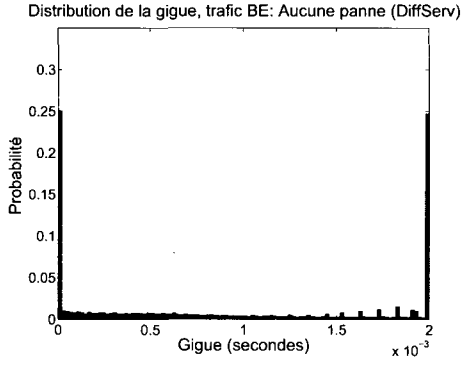

Distribution de la gigue, trafic BE: Aucune panne (DPDSDP)
Probabilité
Gigue (secondes)
x 10^-3

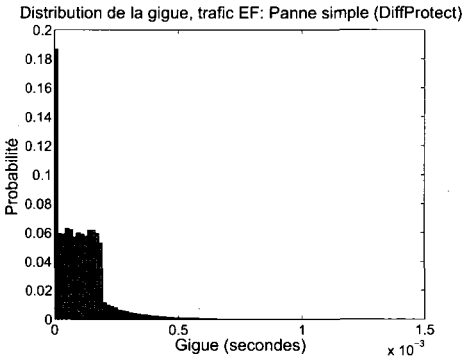

Distribution de la gigue, trafic BE: Aucune panne (DSDPDP)
Probabilité
Gigue (secondes)
x 10^-3

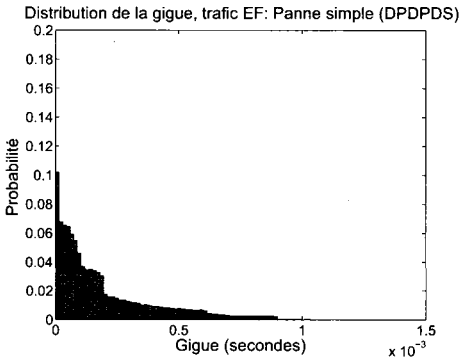

Distribution de la gigue, trafic BE: Aucune panne (DSDPDS)
Probabilité
Gigue (secondes)
x 10^-3

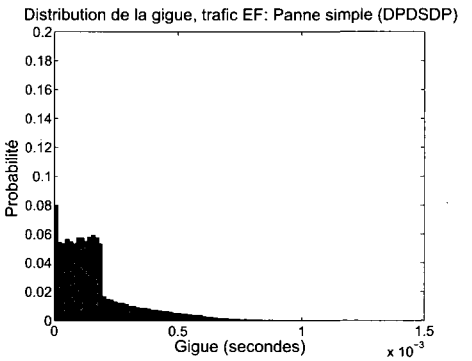

Distribution de la gigue, trafic BE: Aucune panne (DPDSDS)
Probabilité
Gigue (secondes)
x 10^-3

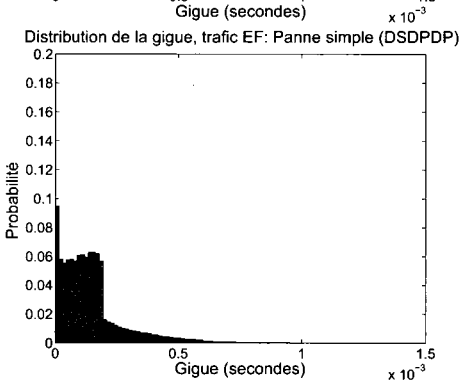

Distribution de la gigue, trafic BE: Aucune panne (DSDSDP)
Probabilité
Gigue (secondes)
x 10^-3

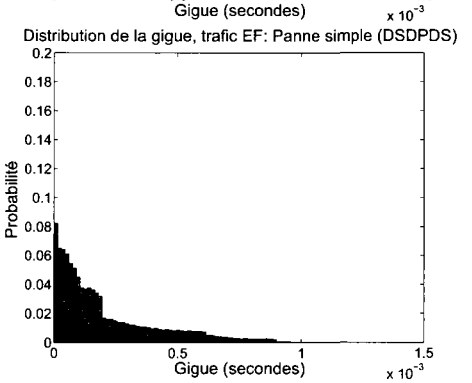

Distribution de la gigue, trafic BE: Aucune panne (DiffServ)
Probabilité
Gigue (secondes)
x 10^-3

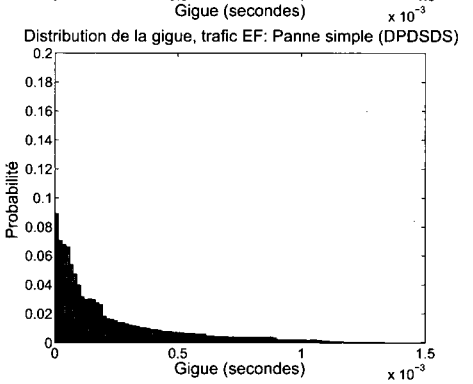

Distribution de la gigue, trafic EF: Panne simple (DiffProtect)
Probabilité
Gigue (secondes)
x 10^-3

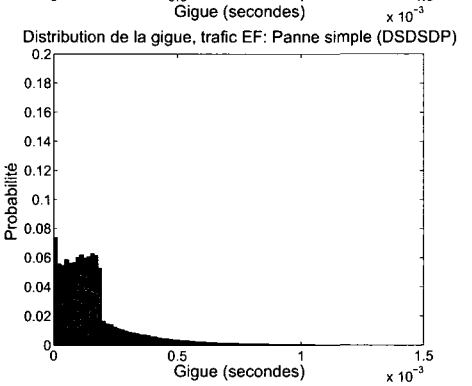

Distribution de la gigue, trafic EF: Panne simple (DPDPDS)
Probabilité
Gigue (secondes)
x 10^-3

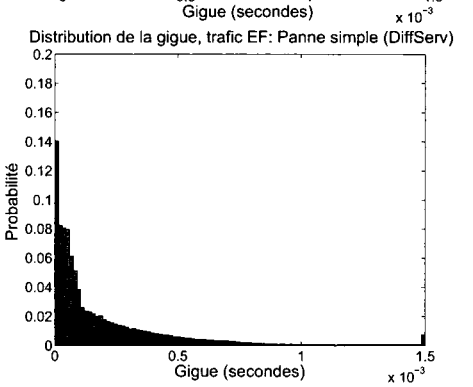

Distribution de la gigue, trafic EF: Panne simple (DPDSDP)
Probabilité
Gigue (secondes)
x 10^-3

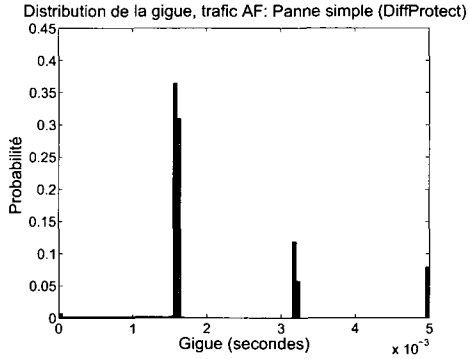

Distribution de la gigue, trafic EF: Panne simple (DSDPDP)
Probabilité
Gigue (secondes)
x 10^-3

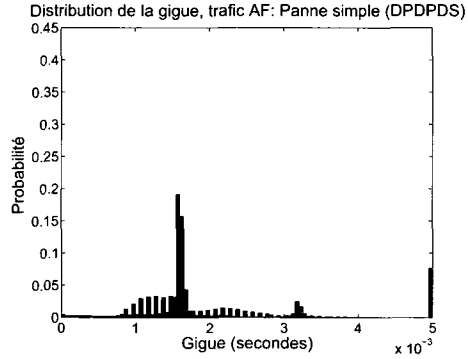

Distribution de la gigue, trafic EF: Panne simple (DSDPDS)
Probabilité
Gigue (secondes)
x 10^-3

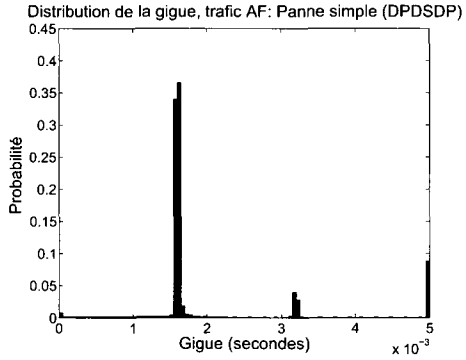

Distribution de la gigue, trafic EF: Panne simple (DPDSDS)
Probabilité
Gigue (secondes)
x 10^-3

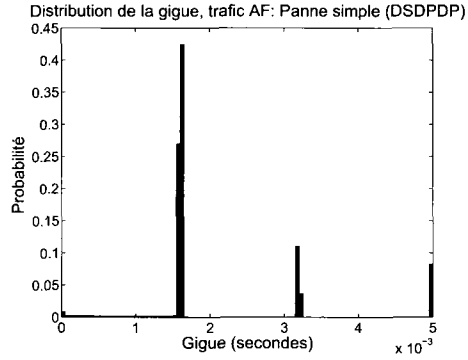

Distribution de la gigue, trafic EF: Panne simple (DSDSDP)
Probabilité
Gigue (secondes)
x 10^-3

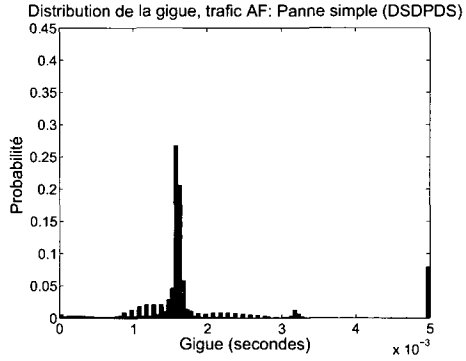

Distribution de la gigue, trafic EF: Panne simple (DiffServ)
Probabilité
Gigue (secondes)
x 10^-3

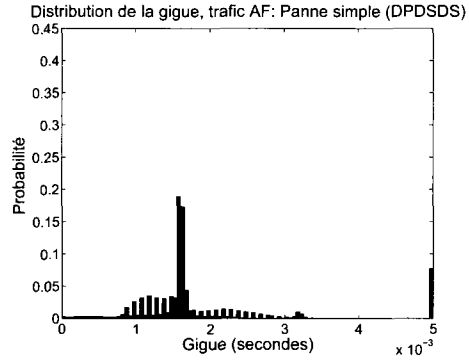

Distribution de la gigue, trafic AF: Panne simple (DiffProtect)
Probabilité
Gigue (secondes)
x 10^-3

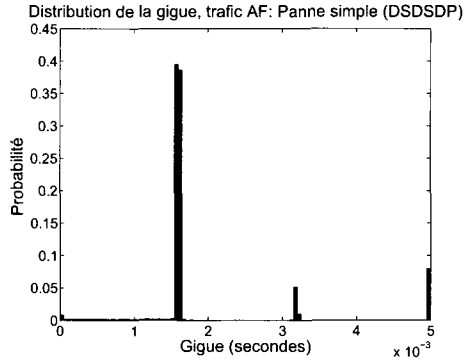

Distribution de la gigue, trafic AF: Panne simple (DPDPDS)
Probabilité
Gigue (secondes)
x 10^-3

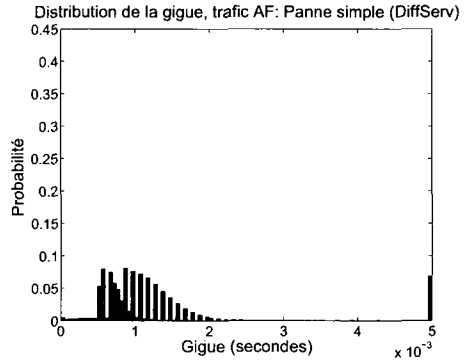

Distribution de la gigue, trafic AF: Panne simple (DPDSDP)
Probabilité
Gigue (secondes)
x 10^-3

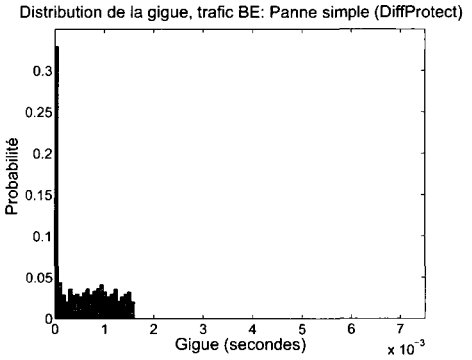

Distribution de la gigue, trafic AF: Panne simple (DSDPDP)
Probabilité
Gigue (secondes)
x 10^-3

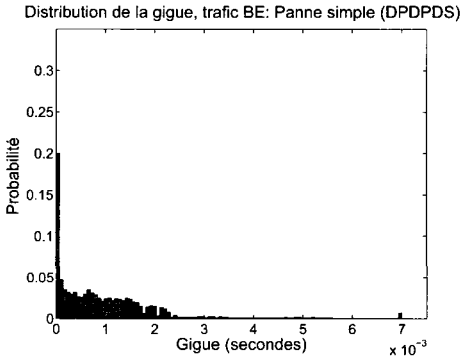

Distribution de la gigue, trafic AF: Panne simple (DSDPDS)
Probabilité
Gigue (secondes)
x 10^-3

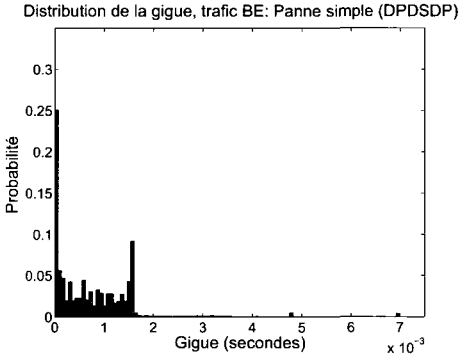

Distribution de la gigue, trafic AF: Panne simple (DPDSDS)
Probabilité
Gigue (secondes)
x 10^-3

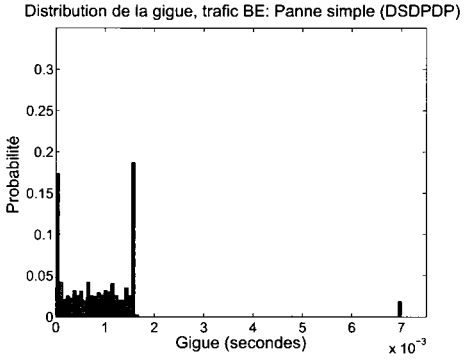

Distribution de la gigue, trafic AF: Panne simple (DSDSDP)
Probabilité
Gigue (secondes)
x 10^-3

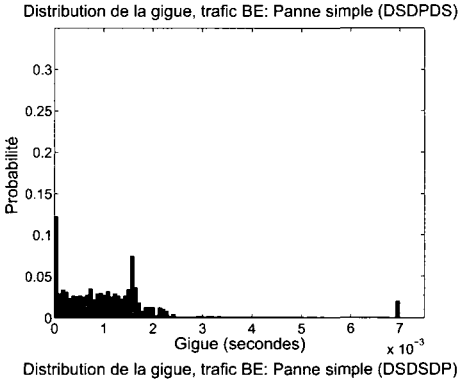

Distribution de la gigue, trafic AF: Panne simple (DiffServ)
Probabilité
Gigue (secondes)
x 10^-3

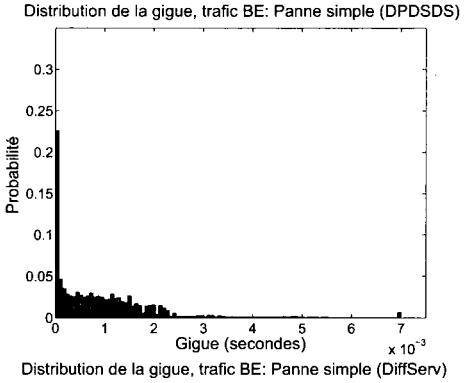

Distribution de la gigue, trafic BE: Panne simple (DiffProtect)
Probabilité
Gigue (secondes)
x 10^-3

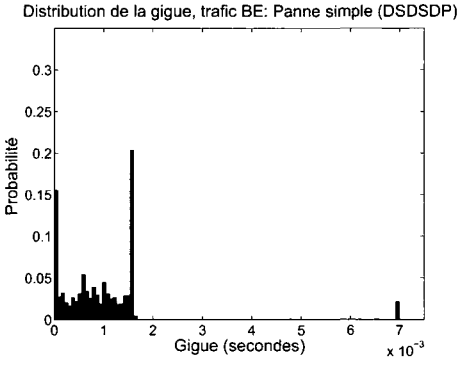

Distribution de la gigue, trafic BE: Panne simple (DPDPDS)
Probabilité
Gigue (secondes)
x 10^-3

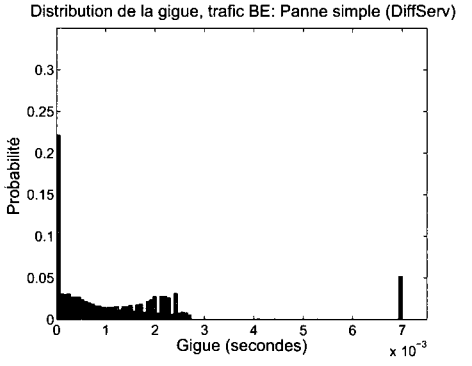

Distribution de la gigue, trafic BE: Panne simple (DPDSDP)
Probabilité
Gigue (secondes)
x 10^-3

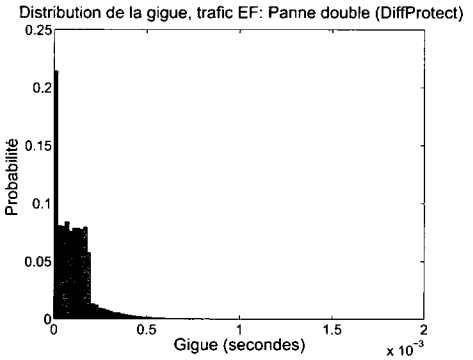

Distribution de la gigue, trafic BE: Panne simple (DSDPDP)
Probabilité
Gigue (secondes)
x 10^-3

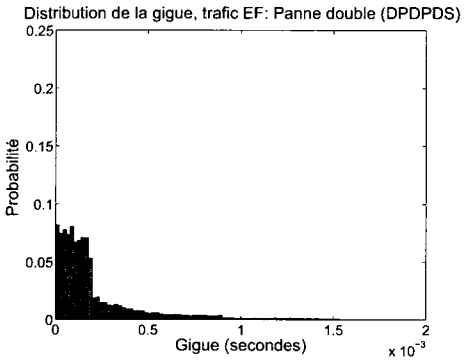

Distribution de la gigue, trafic BE: Panne simple (DSDPDS)
Probabilité
Gigue (secondes)
x 10^-3

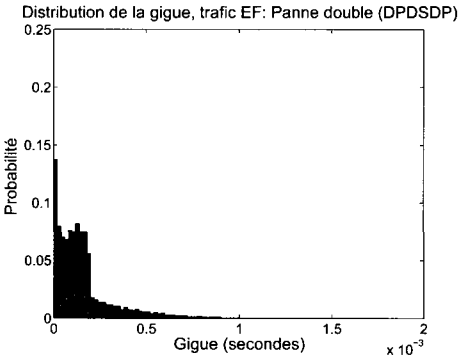

Distribution de la gigue, trafic BE: Panne simple (DPDSDS)
Probabilité
Gigue (secondes)
x 10^-3

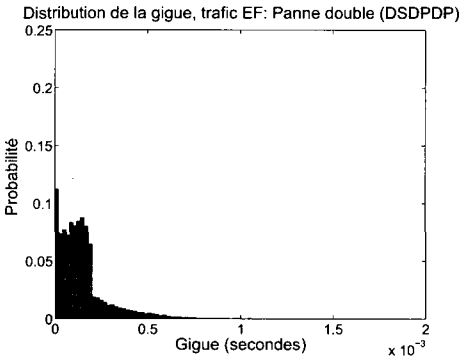

Distribution de la gigue, trafic BE: Panne simple (DSDSDP)
Probabilité
Gigue (secondes)
x 10^-3

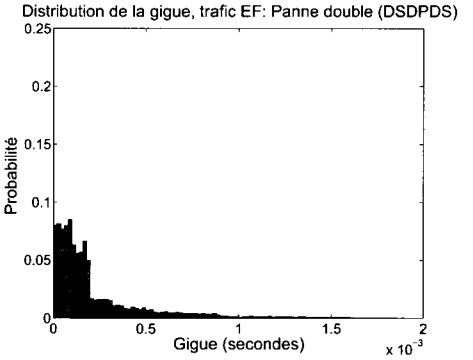

Distribution de la gigue, trafic BE: Panne simple (DiffServ)
Probabilité
Gigue (secondes)
x 10^-3

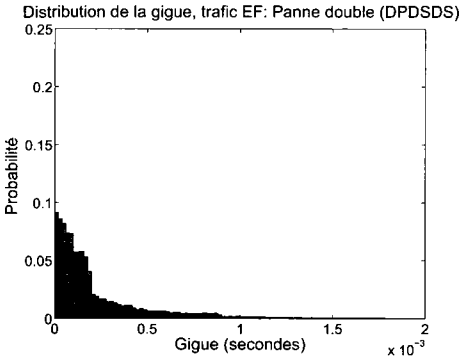

Distribution de la gigue, trafic EF: Panne double (DiffProtect)
Probabilité
Gigue (secondes)
x 10^-3

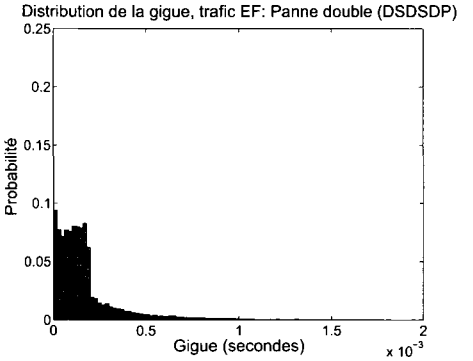

Distribution de la gigue, trafic EF: Panne double (DPDPDS)
Probabilité
Gigue (secondes)
x 10^-3

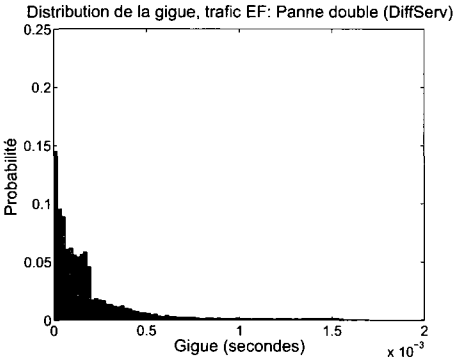

Distribution de la gigue, trafic EF: Panne double (DPDSDP)
Probabilité
Gigue (secondes)
x 10^-3

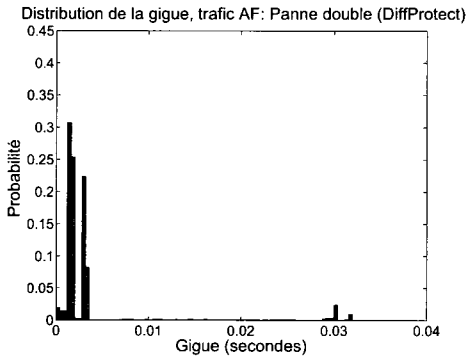

Distribution de la gigue, trafic EF: Panne double (DSDPDP)
Probabilité
Gigue (secondes)
x 10^-3

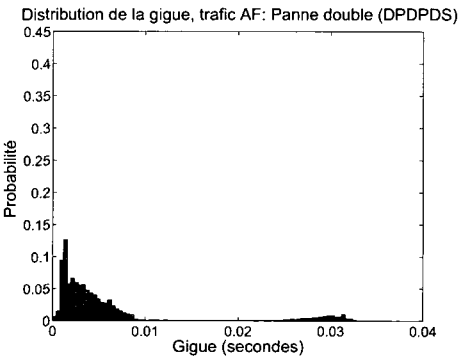

Distribution de la gigue, trafic EF: Panne double (DSDPDS)
Probabilité
Gigue (secondes)
x 10^-3

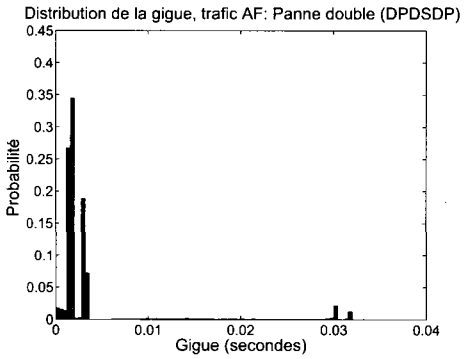

Distribution de la gigue, trafic EF: Panne double (DPDSDS)
Probabilité
Gigue (secondes)
x 10^-3

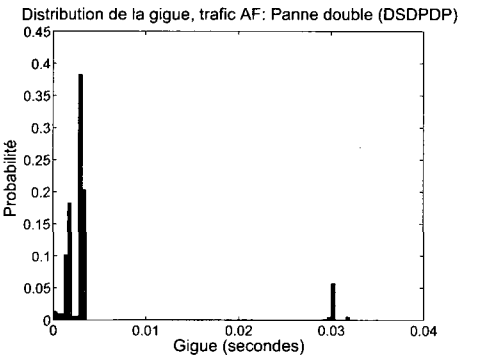

Distribution de la gigue, trafic EF: Panne double (DSDSDP)
Probabilité
Gigue (secondes)
x 10^-3

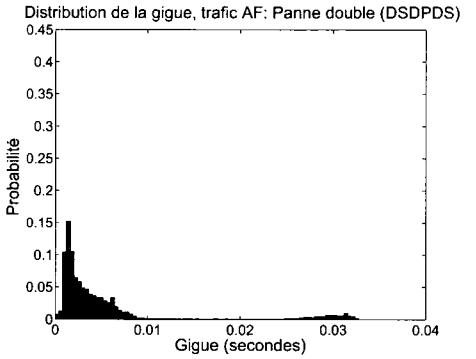

Distribution de la gigue, trafic EF: Panne double (DiffServ)
Probabilité
Gigue (secondes)
x 10^-3

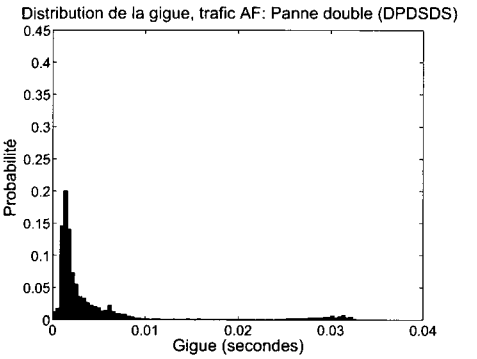

Distribution de la gigue, trafic AF: Panne double (DiffProtect)
Probabilité
Gigue (secondes)

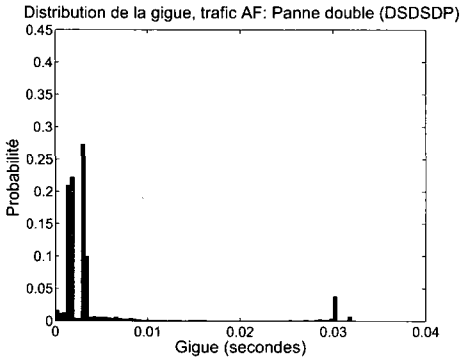

Distribution de la gigue, trafic AF: Panne double (DPDPDS)
Probabilité
Gigue (secondes)

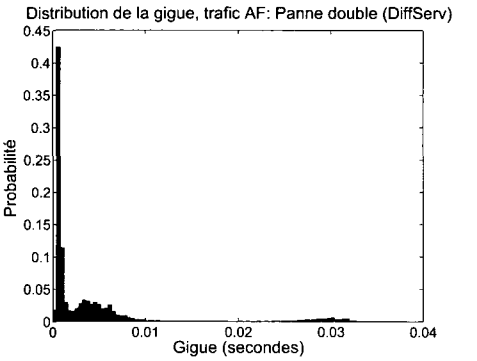

Distribution de la gigue, trafic AF: Panne double (DPDSDP)
Probabilité
Gigue (secondes)

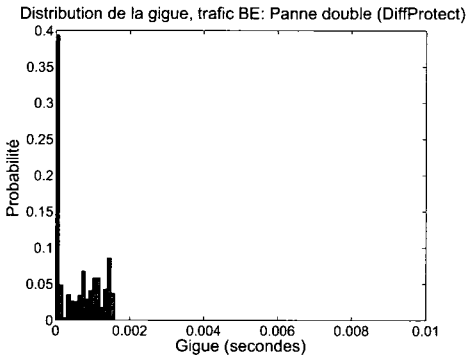

Distribution de la gigue, trafic AF: Panne double (DSDPDP)
Probabilité
Gigue (secondes)

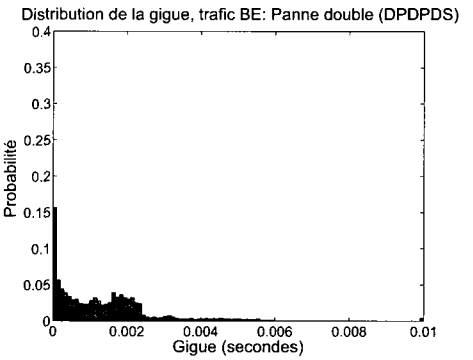

Distribution de la gigue, trafic AF: Panne double (DSDPDS)
Probabilité
Gigue (secondes)

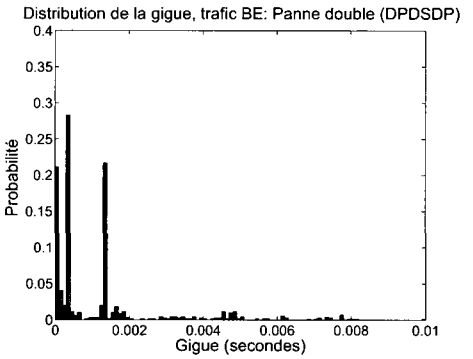

Distribution de la gigue, trafic AF: Panne double (DPDSDS)
Probabilité
Gigue (secondes)

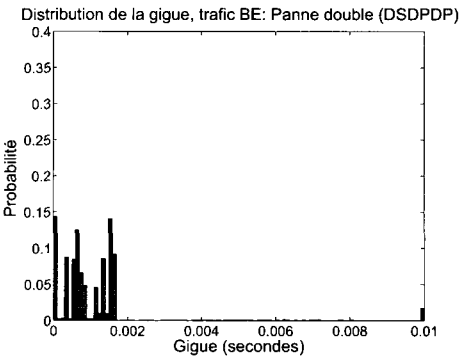

Distribution de la gigue, trafic AF: Panne double (DSDSDP)
Probabilité
Gigue (secondes)

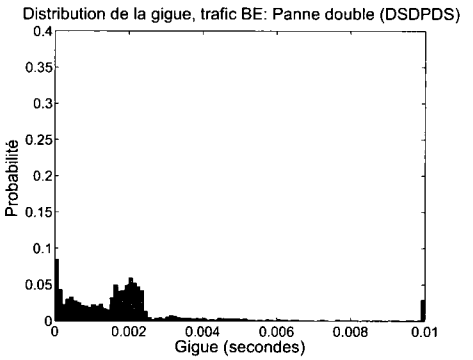

Distribution de la gigue, trafic AF: Panne double (DiffServ)
Probabilité
Gigue (secondes)

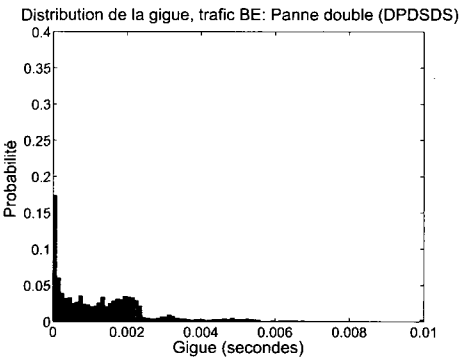

Distribution de la gigue, trafic BE: Panne double (DiffProtect)
Probabilité
Gigue (secondes)

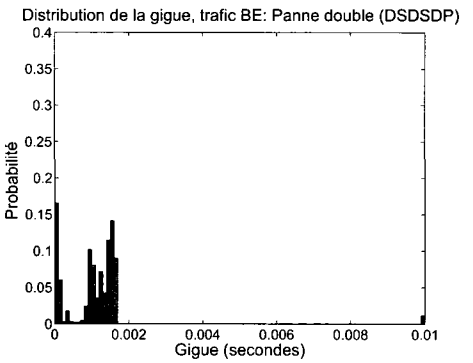

Distribution de la gigue, trafic BE: Panne double (DPDPDS)
Probabilité
Gigue (secondes)

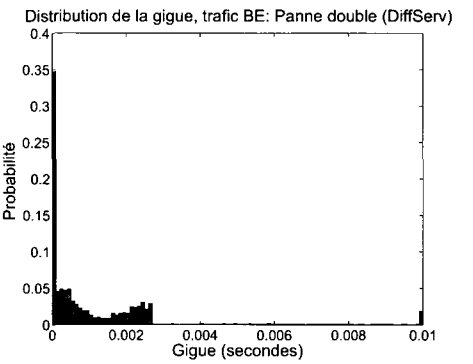

Distribution de la gigue, trafic BE: Panne double (DPDSDP)
Probabilité
Gigue (secondes)


Distribution de la gigue, trafic BE: Panne double (DSDPDP)
Probabilité
Gigue (secondes)


Distribution de la gigue, trafic BE: Panne double (DSDPDS)
Probabilité
Gigue (secondes)


Distribution de la gigue, trafic BE: Panne double (DPDSDS)
Probabilité
Gigue (secondes)


Distribution de la gigue, trafic BE: Panne double (DSDSDP)
Probabilité
Gigue (secondes)


Distribution de la gigue, trafic BE: Panne double (DiffServ)
Probabilité
Gigue (secondes)

ANNEXE III

ROUTAGE PAR DEFLEXION POUR DIFFSERV

L'architecture DiffServ a été proposée comme méthode extensible pour offrir, en cas de congestion, une qualité de service différenciée à différents types de trafics. Chaque trafic est privilégié suivant sa priorité, les trafics de hautes priorités (EF et AF) ont la garantie d'un accès immédiat au lien à la congestion et ce au détriment du trafic de basse priorité (BE). Le trafic BE est le premier à être mis en attente et rejeté dès les premiers signes de congestion. En nous inspirant du modèle de routage par déflexion proposé pour les Optical Burst Networks (OBS), nous voulons explorer la possibilité de munir les routeurs DiffServ de fonctionnalités similaires.

III.1 Routage par déflexion et réseaux OBS

Dans les réseaux de commutation par rafales optiques (Optical Burst Switching ou (OBS)), les paquets d'informations sont agrégés ensemble pour former des rafales de grande taille. Chaque rafale est précédée d'un paquet de contrôle qui a pour rôle d'indiquer aux OXC parcourus par la rafale de réserver les ressources nécessaires pour la transmission de cette dernière. L'étude de l'utilisation de OBS dans la transmission des réseaux optiques prend plus en plus d'importance. Cette augmentation est due au fait qu'elle permet d'éviter de dédier une longueur d'onde de bout en bout pour chaque connexion. Un problème critique des réseaux OBS est de minimiser le taux de blocage des rafales (Lee et al., 2003). La réservation et la transmission d'une rafale se font noeud par noeud, un noeud intermédiaire peut facilement bloquer la transmission d'une rafale s'il ne possède pas les ressources nécessaires à l'arrivée de cette dernière ou s'il est averti trop tard.

Le concept de routage par déflexion est connu pour être une bonne solution qui réduit le taux de blocage dans les réseaux OBS. Considérons l'exemple de la figure III.1. Deux rafales sont préparées simultanément, l'une à l'OXC A en destination de D (rafale $\{A, D\}$), l'autre à l'OXC B en destination de D (rafale $\{B, D\}$). Les plus courts chemins établis pour $\{A, D\}$ et $\{B, D\}$ sont respectivement $[A, C, D]$ et $[B, C, D]$. Comme l'indique la figure III.1, un paquet de contrôle a suivi de $\{A, D\}$ arrive en premier au noeuds C. Le rôle du paquet de contrôle a est d'informer C de l'arrivée du rafale $\{A, D\}$, C réserve les ressources du lien $[C, D]$ pour être utilisées par $\{A, D\}$. À l'arrivée du paquet de contrôle b au noeud C, le lien $[C, D]$ est déjà réservé pour $\{A, D\}$ et ne peut être utilisé par $\{B, D\}$. Le noeud C n'a pas la choix que de bloquer $\{B, D\}$ et de demander à la couche logique de B de le retransmettre subséquemment. Le concept de routage par déflexion permettre à C de détecter la présence d'un autre chemin non utilisé, dans ce cas $[C, E]$ et de dévier temporairement la trajectoire de $\{B, D\}$ sur le lien $[C, E]$. $\{B, D\}$ parcourra le chemin $[B, C, E, D]$ au lieu du chemin $[B, C, D]$. Certes, il sera reçu à destination avec un léger retard, cependant ceci constitue une meilleure option que de bloquer au niveau du noeud C et de demander sa retransmission. Plusieurs travaux de recherche ont été proposés pour optimiser le fonctionnement du routage par déflexion dans les réseaux OBS, (Hsu et al., 2002), (Chen and Wang, 2003) et (Wang et al., 2005) en sont des exemples. Une évaluation de performance des réseaux IP-optiques avec capacités de routage par déflexion est évaluée dans (Pattavina, 2005). Ainsi, la littérature montre qu'étant donné que les OXC sont incapables de stocker l'information photonique reçue, le concept de routage par déflexion est une meilleure alternative au blocage du flot quand les ressources dont en manque sur le chemin principal.

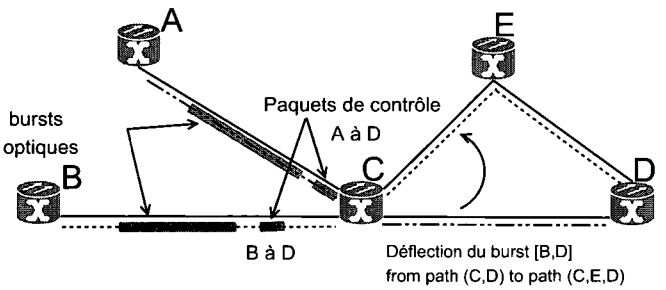


FIG. III.1 Routage par déflexion dans les réseaux OBS.

III.2 Routage par déflexion pour DiffServ

L'idée sera d'explorer la possibilité d'adopter le routage par déflexion à la couche logique (IP) des réseaux, et plus spécifiquement, dans les routeurs à capacité DiffServ de cette couche. Dans un réseau DiffServ, le trafic BE est le premier à souffrir des conséquences, parfois désastreuses, de la congestion des liens de transmissions logique. La congestion peut causer un ralentissement considérable et même une interruption du service.

Supposons l'existence de deux flots de trafic et considérons l'exemple de la figure III.2. Les deux flots sont constitués des trois priorités de trafic, EF, AF et BE. Le premier flot généré par A, en destination de C, est routé sur son plus court chemin (A, B, C). Le second, généré par D, en direction de C est routé sur son plus court chemin (D, E, C). Une augmentation soudaine du trafic généré par A met B en état de congestion, il ne peut simplement pas acheminer la totalité du trafic généré par A sur le lien (B, C). Les mécanismes DiffServ de protection contre la congestion s'activent. Le trafic de BE arrivant à B sera mis en attente et éventuellement rejeté. L'option de routage par déflexion permet au routeur B de :

- Détecter la congestion du lien (B, C).
- Sonder tous ses ports de sortie dans l'éventualité de trouver un autre chemin non ou moins congestionné.

– Dévier temporairement les paquets BE qui débordent sur un autre chemin à priori non congestionné (chemin (B, E, C)).

L'état des files d'attentes RED (Random Early Detection) des ports de sortie du routeur B permet à ce dernier de détecter l'état de congestion de chacun de ses liens de sortie. Nous supposons la présence d'un module de déflexion séparé qui se charge de recueillir les paquets BE rejetés au niveau du lien (B, C), sonder l'état des autres ports de sorties du même routeur. Renvoyé les paquets BE recueillis sur un ou plusieurs autres chemins moins congestionnés.

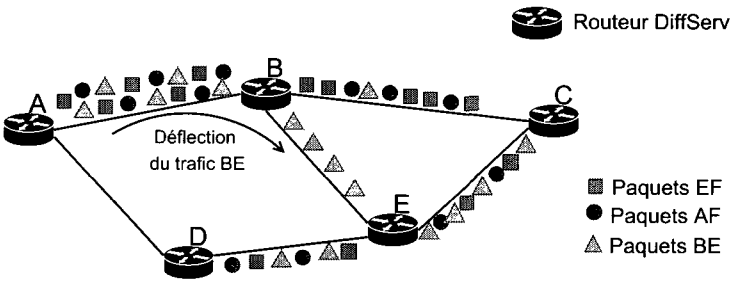


FIG. III.2 Routage par déflexion dans les réseaux DiffServ.

Dans le cas de l'exemple de la figure III.1, les paquets BE refusés au niveau du lien (B, C) sont déviés et renvoyés sur le lien (B, E). Les paquets BE se mêleront avec ceux du deuxième flot considéré dans ce système. En outre, ils seront transmis sur le lien de sorti (E, C). Le trafic BE excédant est de basse priorité, il ne pourra affecter que les flots BE de même priorité.

Si la surcharge des paquets BE ne cause pas de congestion au lien (E, C), les paquets BE excédentaires arriveront, avec un léger retard à destination. Le taux de perte des paquets BE sera ainsi réduit. Si (E, C) est déjà congestionné, les paquets BE non rejetés au niveau de B, le seront au niveau de E. Dans ce cas, la performance moyenne du réseau DiffServ n'est pas améliorée, mais elle ne sera pas réduite.

Un sujet similaire au routage par déflexion est abordé dans (Patek et al., 2001). Un al-

gorithme de routage simple est proposé. Les routeurs de bord d'un réseau DiffServ sont capables de dévier une portion d'un flot de paquets non marqués de son chemin original congestionné vers un chemin secondaire peu utilisé. Les routeurs se basent sur une rétroaction continuelle de la part du réseau sur son état de congestion. Notre approche est différente. Chaque routeur, de bord (edge) ou de coeur (core) est doté des capacités de déflexions. Le routeur DiffServ détecte les pertes de paquets BE sur l'un de ses liens de sorties, récupère une partie des paquets rejetés et les transmet sur un ou plusieurs chemins secondaires. La retransmission est immédiate et temporaire et n'affecte que les paquets BE déjà rejetés. Cette étude peut être étendue pour inclure la déflexion d'une portion des paquets de hautes priorités (EF et AF) d'un lien congestionné vers un autre chemin moins utilisé. Une approche similaire est proposée dans (Zarifzadeh et al., 2004). Les auteurs proposent un algorithme de routage à chemins multiples du trafic de haute priorité dans un réseau DiffServ. Par sa nature prioritaire, la charge du trafic EF affecte grandement la performance fournie aux trafics de priorités inférieures. Les auteurs proposent un algorithme pour la distribution efficace d'un flot de trafic prioritaire sur plusieurs autres chemins en but de garantir une meilleure performance aux autres classes de flots.

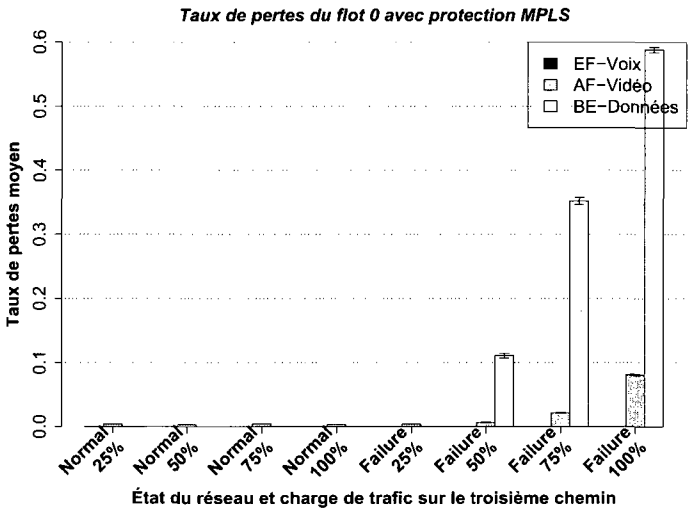
III.3 DiffServ, DiffProtect et routage par déflexion

L'idée de routage par déflexion prend beaucoup d'envergure quand elle est combinée avec les modèles de protection différenciée proposée par ce projet. Une panne de chemin optique dans le modèle DiffServ entraîne une diminution considérable de bande passante au niveau IP. Une congestion en résulte, les paquets BE sont les premiers à souffrir des conséquences. Les simulations montrent des taux de pertes très élevés. Dans le modèle DiffProtect, le taux de perte des paquets BE est de 100% si une panne affecte le chemin optique qui transporte ce trafic. Le routage par déflexion permettra de dévier les paquets BE du lien affecté par une panne à un autre chemin fonctionnel et probablement améliorer

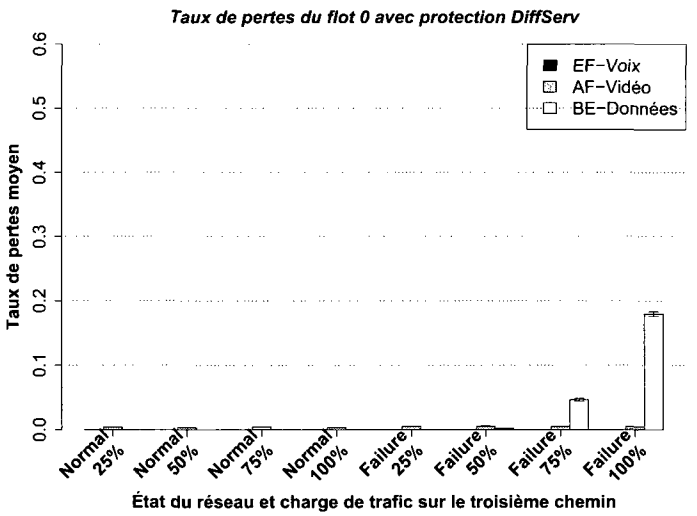
la QoS fournie au trafic BE. Nos modèles de protection différenciée permettent de privilégier les trafics de hautes priorités en cas de panne, l'addition du concept de routage par déflexion équilibrera la balance en terme de protection additionnelle du trafic de basse priorité contre les pannes optiques.

ANNEXE IV

PERFORMANCE DES FLOTS 0, 1 ET 2

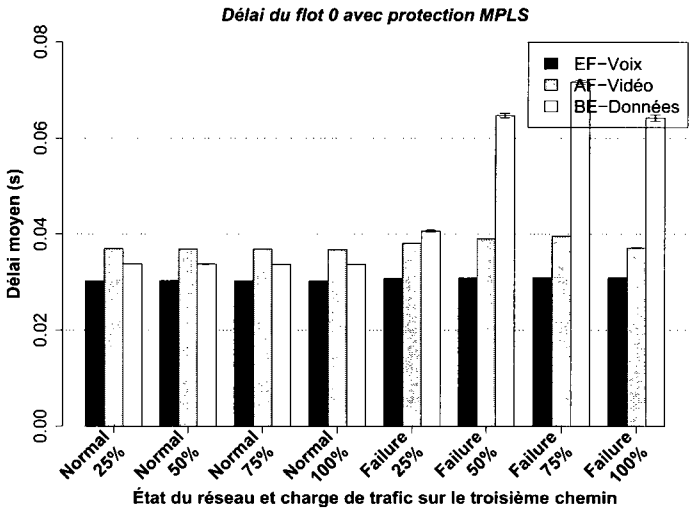


(a) Normal vs Panne, Protection MPLS

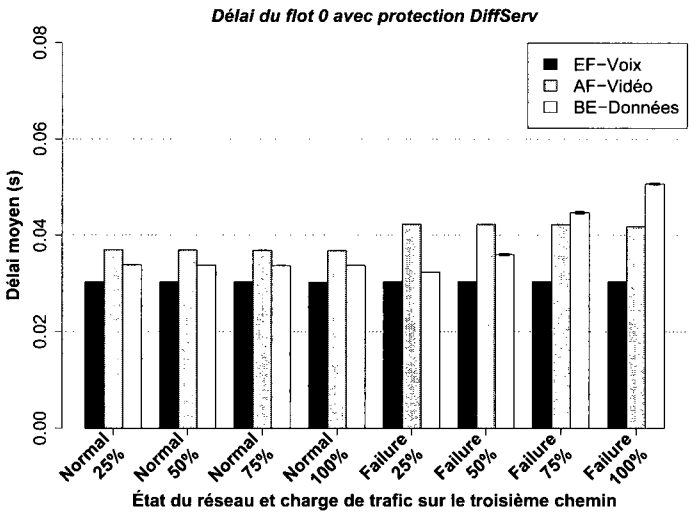


(b) Normal vs Panne, Protection DiffServ*

FIG. IV.1 Taux de pertes du flot 0

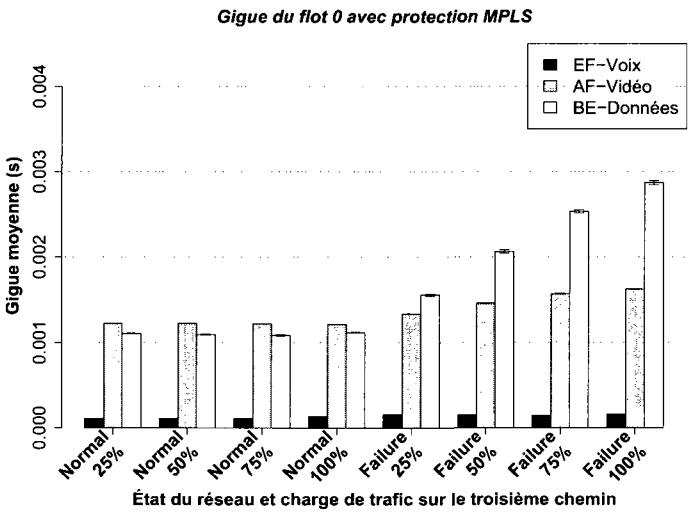


(a) Normal vs Panne, Protection MPLS

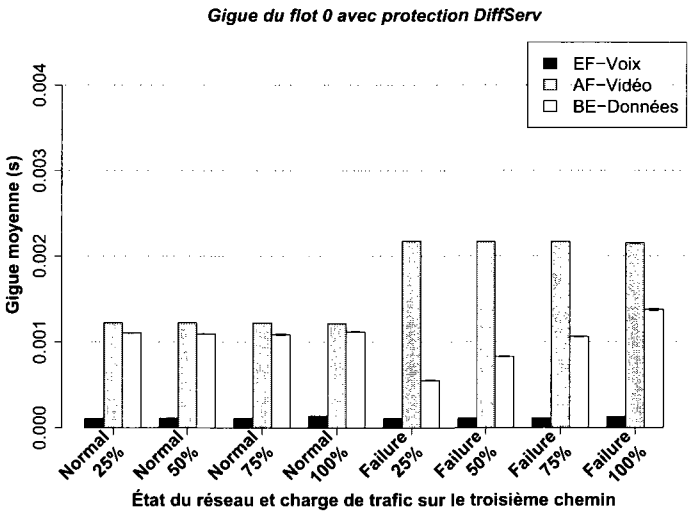


(b) Normal vs Panne, Protection DiffServ*

FIG. IV.2 Délai moyen du flot 0

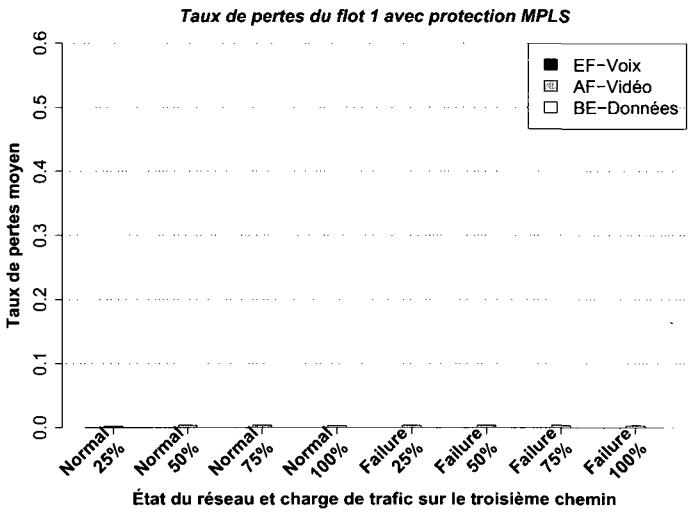


(a) Normal vs Panne, Protection MPLS

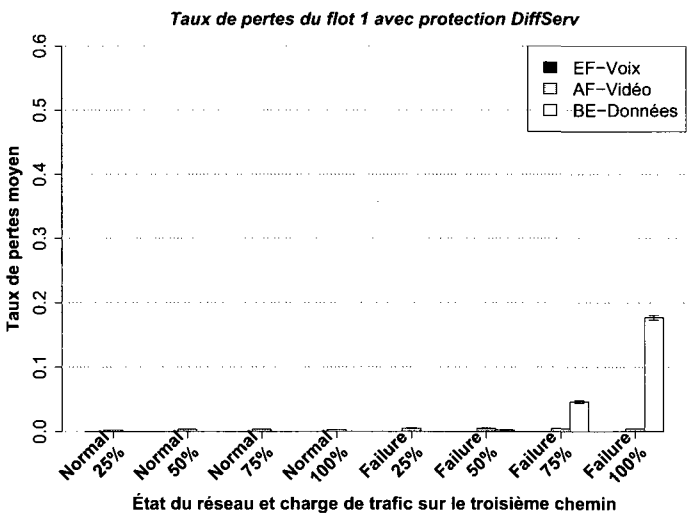


(b) Normal vs Panne, Protection DiffServ*

FIG. IV.3 Gigue moyenne du flot 0

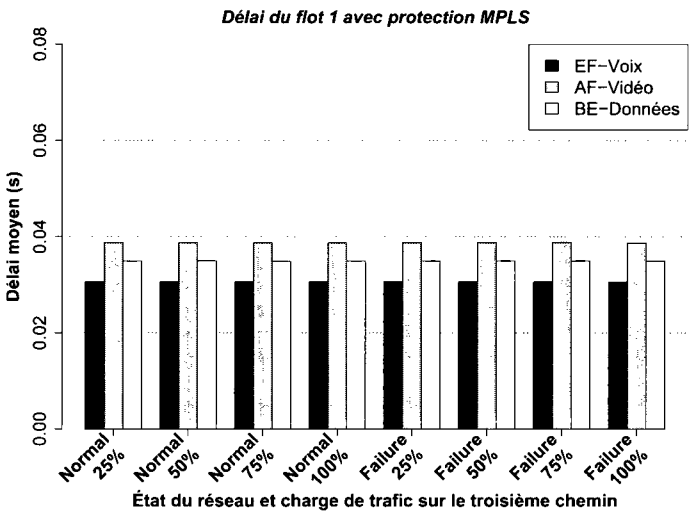


(a) Normal vs Panne, Protection MPLS

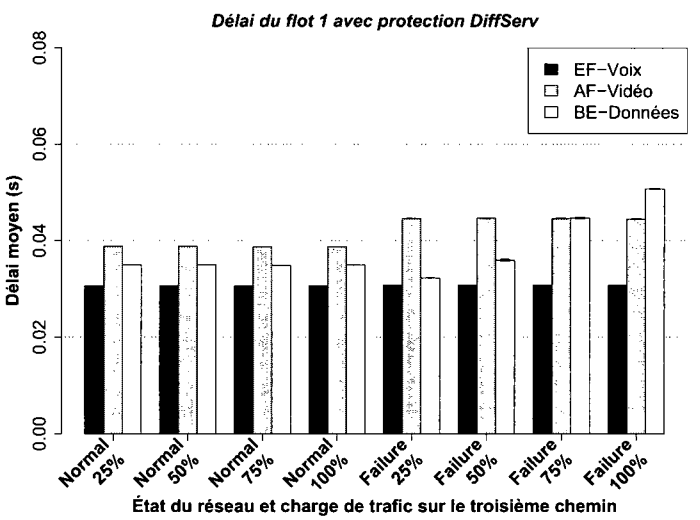


(b) Normal vs Panne, Protection DiffServ*

FIG. IV.4 Taux de pertes du flot 1

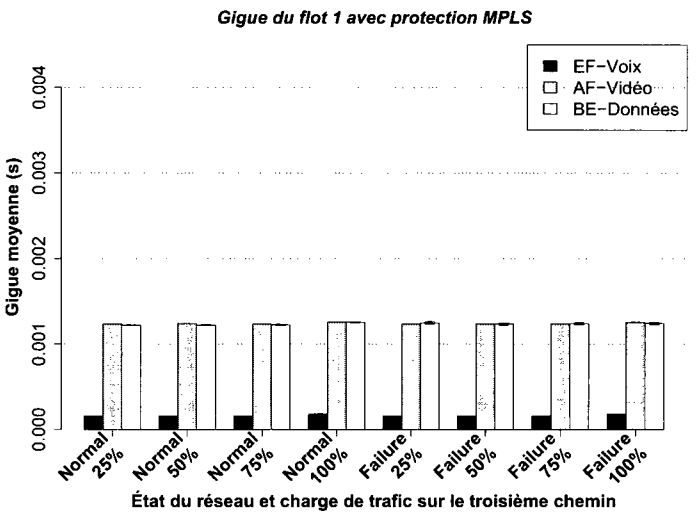


(a) Normal vs Panne, Protection MPLS

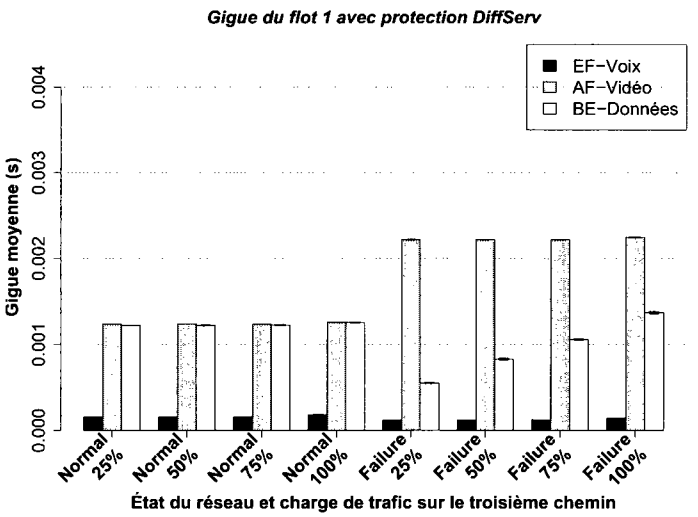


(b) Normal vs Panne, Protection DiffServ*

FIG. IV.5 Délai moyen du flot 1

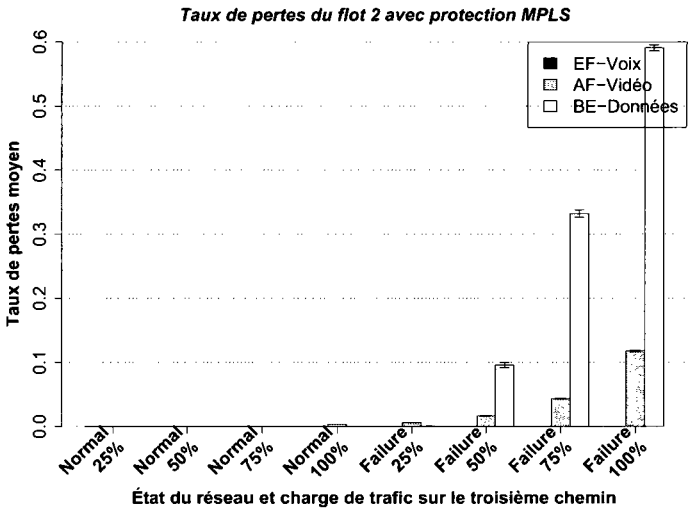


(a) Normal vs Panne, Protection MPLS

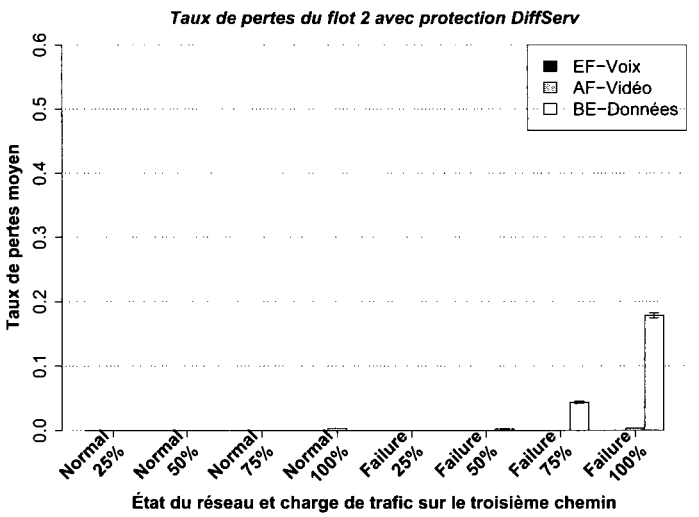


(b) Normal vs Panne, Protection DiffServ*

FIG. IV.6 Gigue moyenne du flot 1

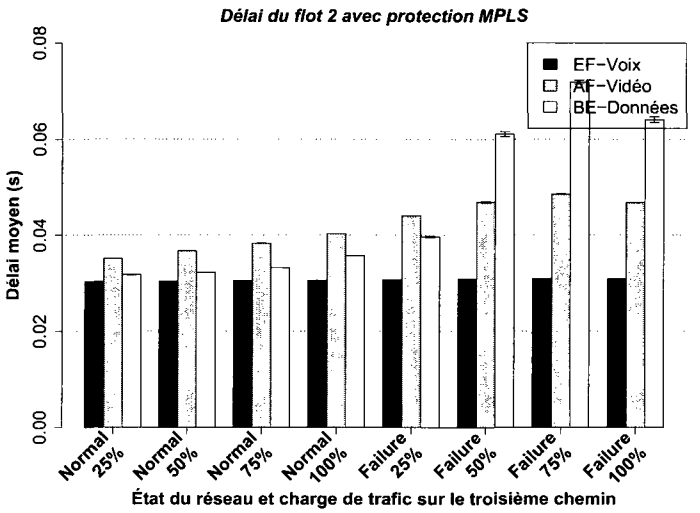


(a) Normal vs Panne, Protection MPLS

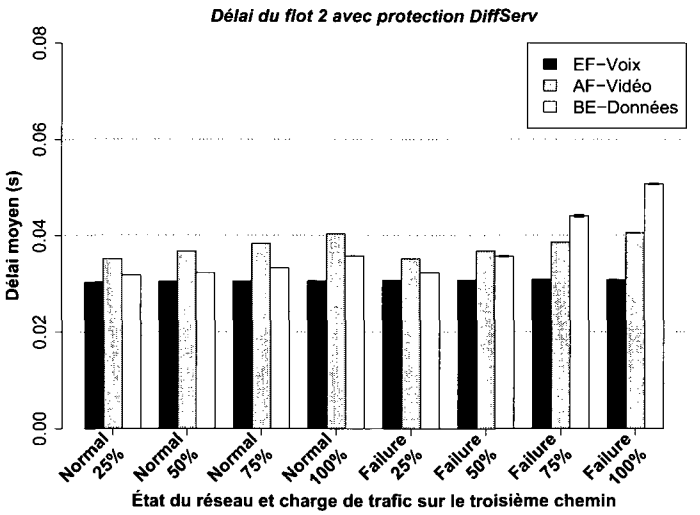


(b) Normal vs Panne, Protection DiffServ*

FIG. IV.7 Taux de pertes du flot 2

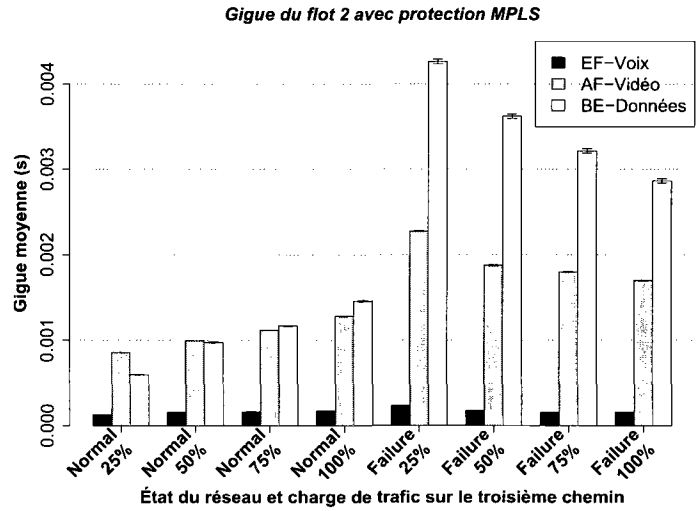


(a) Normal vs Panne, Protection MPLS

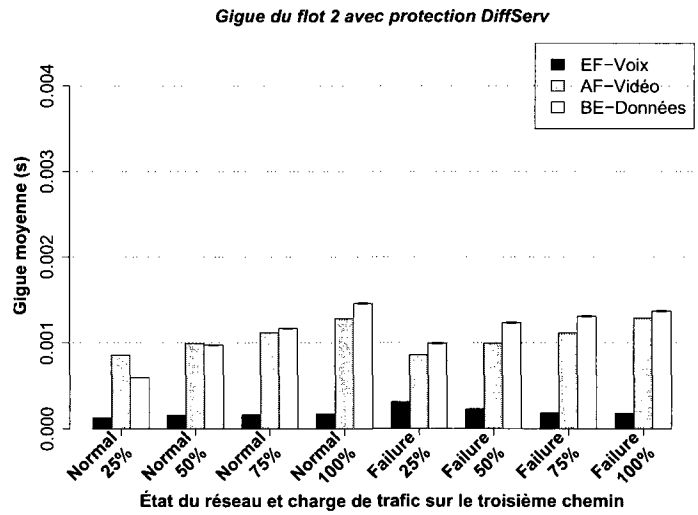


(b) Normal vs Panne, Protection DiffServ*

FIG. IV.8 Délai moyen du flot 2



(a) Normal vs Panne, Protection MPLS



(b) Normal vs Panne, Protection DiffServ*

FIG. IV.9 Gigue moyenne du flot 2

ANNEXE V

CONFIGURATION DES COMMUTATEURS

Les numéros des ports UDP destination de tous les paquets de voix sur IP sont de 10000 à 10999, ceux d'AF sont de 11000 à 11999 et ceux de BE sont entre 12000 et 12999. La classification EF, AF et BE du trafic se fait en fonction du numéro du port UDP destination de chaque flot. Les commandes suivantes font en sorte que les paquets de VoIP appartiennent tous à la liste d'accès 100 ; 101 est réservée pour le trafic vidéo et 102 utilisée par les paquets de données.

```
access-list 100 permit udp any any range 10000 10999
access-list 101 permit udp any any range 11000 11999
access-list 102 permit udp any any range 12000 12999
```

Tous les paquets de la liste d'accès 100 sont associés à la classe EF, ceux de la liste 101 à la classe AF et le reste, les paquets de liste 102 sont associés à la classe BE.

```
class-map match-all AFclass
match access-group 101
class-map match-all BEclass
match access-group 102
class-map match-all EFclass
match access-group 100
```

Nous définissons par la suite deux politiques de marquage. L'une, *inPol* est utilisé par les interfaces 1 à 6 de Atlas et attribut les DSCP appropriés aux classes de trafic définies précédemment. L'autre *ECin* est utilisée par les interface 22, 23 et 24 de l'Etherchannel et

spécifie à celles-ci de faire confiance aux DSCP des paquets donc de ne pas modifier leur classification dans cette partie du réseau.

```
policy-map inPol
class EFclass
set dscp ef
class AFclass
set dscp af41
class BEclass
set dscp default

policy-map ECin
class EFclass
trust dscp
class AFclass
trust dscp
class BEclass
trust dscp
```

Les prochaines commandes sont des instructions de configuration globale de la différenciation de services dans le commutateur. Chaque port de communication possède deux files d'attentes en entrée et quatre en sortie. L'ordonnancement des files d'entrées est prioritaire, le trafic EF utilise la première file et les classes AF et BE sont associées à la deuxième file. En sortie, le trafic EF est associé à la file 1 prioritaire, notre trafic vidéo AF est associé à la file 3, le trafic BE à la file 4 et la file 2 n'est pas utilisée.

```
mls qos srr-queue input bandwidth 1 3
mls qos srr-queue input buffers 60 40
mls qos srr-queue input priority-queue 2 bandwidth 0

mls qos srr-queue output dscp-map queue 3 threshold 1 34
mls qos srr-queue output dscp-map queue 4 threshold 1 0
mls qos queue-set output 2 buffers 20 5 25 50
mls qos
```

Les prochaines commandes créent l'interface Etherchannel, lui donnent l'adresse 10.0.0.1, spécifient la technique de partage de charge et y ajoutent les interfaces 22, 23 et 24 de commutateur Atlas. Nous pouvons voir que les interfaces fonctionnent à 100 Mbps chacune en mode full duplex. La file de sortie est servie toujours en priorité et étant donné que la file 2 n'est pas utilisée, la file 3 obtient $60/60 + 20 = 75\%$ de la capacité de transmission restante, la file 4 du trafic BE est la moins prioritaire avec 25% de la capacité qui reste après le service de trafic EF.

```
interface Port-channel1
no switchport
ip address 10.0.0.1 255.0.0.0

port-channel load-balance src-dst-ip

interface GigabitEthernet1/0/22 - 1/0/23 - 1/0/24
no switchport
no ip address
speed 100
duplex full
srr-queue bandwidth share 10 10 60 20
srr-queue bandwidth shape 20 0 0 0
queue-set 2
priority-queue out
channel-group 1 mode active
service-policy input ECin
```

Les prochaines commandes permettent de configurer l'adressage IP et le protocole de routage IP utilisé. Les interfaces 1 à 6 utilisent la politiques $inPol$ qui permet de classifier correctement le trafic qui arrive du réseau A.

```
hostname Atlas

ip routing

ip dhcp pool network1_pool
network 172.136.0.0 255.255.0.0
default-router 172.136.0.1
lease infinite

ip dhcp snooping vlan 10
vlan internal allocation policy ascending
interface Vlan10
ip address 172.136.0.1 255.255.0.0

router rip
network 10.0.0.0
network 172.136.0.0

interface GigabitEthernet1/0/1 à 1/0/6
switchport access vlan 10
switchport mode access
srr-queue bandwidth share 10 10 60 20
srr-queue bandwidth shape 20 0 0 0
mac-address-table aging-time 0 vlan 1
queue-set 2
priority-queue out
service-policy input inPol
ip dhcp snooping trust
```